



SITRAIN

Digital Industry
Academy

Programmation
avec

STEP 7 Safety du
TIA Portal

Cours TIA-SAFETY

Nom: _____

Cours du: _____ au: _____

Formateur: _____

Lieu: _____

Le présent document est un support de formation.

SIEMENS ne garantit aucunement son contenu.

La transmission ou la duplication du document ainsi que l'exploitation ou la communication de son contenu sont interdites, sauf autorisation expresse. Toute infraction est passible de dommages et intérêts.

Copyright © Siemens AG 2020. Tous droits réservés, notamment en cas de dépôt d'un brevet/ou de tout autre droit de protection de la propriété industrielle.

Offre de formation SITRAIN sur Internet : www.siemens.de/sitrain

Version du cours : V16.00.01

(pour STEP 7 V16 Safety Advanced)

Modif MC 28/09/2020

1. Normes

2. Présentation des équipements

3. Principe de fonctionnement Safety Integrated

4. Station de travail et configuration matérielle

5. Raccordement capteur/actionneur

6. Programmation

7. Communication de sécurité

8. Temps de réaction

9. Réception d'une installation

10. Maintenance et diagnostic

11. Annexe: Migration

12. Formation et Support

Table des matières

1.	Présentation des normes et des directives en vigueur	1-2
1.1.	Cadre législatif de l'UE.....	1-3
1.2.	Définition d'un fabricant de machines	1-4
1.3.	Présentation des directives en vigueur	1-5
1.4.	Choix de la ou des directives	1-6
1.5.	Normes de sécurité internationales	1-7
1.5.1.	Normes harmonisées	1-9
1.5.2.	La hiérarchie des normes de sécurité	1-10
1.6.	Exemple de machine « Étiqueteuse »	1-11
1.7.	Mise en œuvre de la directive Machines ± Application à une étiqueteuse	1-12
1.8.	Processus d'appréciation du risque selon EN ISO 12100	1-13
1.8.1.	Étape 1 : Déterminer les limites de la machine	1-14
1.8.2.	Étape 2 : Identifier les phénomènes dangereux	1-16
1.8.3.	Étape 3 : Estimer le risque	1-19
1.8.4.	Étape 4 : Évaluer le risque	1-23
1.8.5.	Résumé	1-27
1.9.	Réduction du risque selon EN ISO 12100	1-28
1.9.1.	Étape 1 : Conception sûre	1-29
1.9.2.	Étape 2 : Mesures de protection techniques	1-31
1.9.3.	Étape 3 : Information des utilisateurs sur les risques résiduels	1-43
1.9.4.	Résumé	1-44
1.10.	Attestation de conformité	1-45
1.10.1.	Évaluation de la conformité	1-46
1.10.2.	Contenu de la déclaration CE de conformité	1-47
1.11.	Résumé	1-48
1.12.	Annexe	1-49
1.12.1.	La directive européenne Machines	1-50
1.12.2.	Formations sur les normes	1-51
1.13.	Solutions possibles aux exercices 1 à 8	1-52
1.13.1.	Exercice 1	1-53
1.13.2.	Exercice 2	1-54
1.13.3.	Exercice 3	1-55
1.13.4.	Exercice 4	1-56
1.13.5.	Exercice 5	1-57
1.13.6.	Exercice 6	1-58
1.13.7.	Exercice 7	1-59
1.13.8.	Exercice 8	1-60

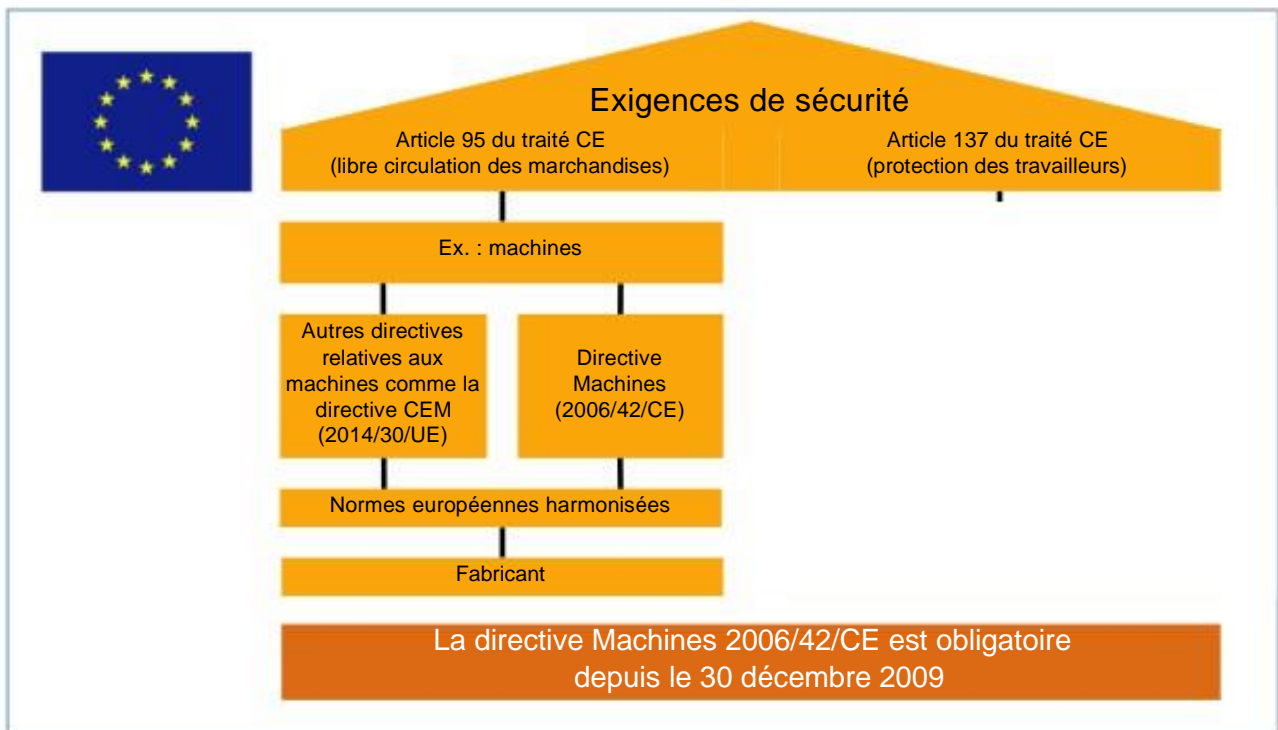
1. Présentation des normes et des directives en vigueur

→ l'issue de la formation, le participant au stage

... connaîtra les étapes nécessaires pour pouvoir concevoir une machine sûre.



1.1. Cadre législatif de l'UE



Lors de l'exploitation de machines, deux grands aspects juridiques doivent être considérés : la protection des travailleurs et le marché intérieur.

Protection des travailleurs (zone grisée) :

L'employeur doit mettre en œuvre les mesures de sécurité nécessaires pour la commande et l'exploitation des machines :

- Éclairage suffisant
- Aspiration
- Sols antidérapants
- Formation des utilisateurs
- Équipements de sécurité tels que vêtements de protection

Ces thèmes ne seront pas abordés dans le cadre de ce cours.

Marché intérieur :

Les machines mises en circulation sur le marché intérieur de l'Union européenne doivent répondre aux exigences de la directive Machines. La directive Machines actuellement en vigueur est la directive 2006/42/CE, qui a remplacé la précédente directive 98/37/CE.

Cette directive est également applicable dans les États de l'AELE (Association Européenne de Libre-Echange) et la Turquie.

La directive Machines actuelle est essentiellement axée sur les machines. Elle ne prend pas en compte des installations techniques comme les téléphériques ou les appareils médicaux.

Normes harmonisées :

Les normes harmonisées sont des normes européennes particulières élaborées par un organisme de normalisation européen (CEN, CENELEC ou ETSI) à la demande de la Commission européenne et de l'AELE. Elles sont rédigées dans le cadre d'un « mandat de normalisation » et publiées au Journal Officiel de l'Union européenne.

Remarque importante : le respect de normes harmonisées apporte une « présomption de conformité » à la directive correspondante ; le constructeur de machines doit alors simplement démontrer qu'il a respecté les exigences des normes harmonisées.

1.2. Définition d'un fabricant de machines

Est considéré comme fabricant de machines toute personne physique ou morale qui ..

1

... est responsable de la conception et de la fabrication d'une machine visée par la directive et qui commercialise cette machine en son nom. Il s'agit généralement d'un **constructeur de machines**, d'un **équipementier** ou encore d'un **ensemblier industriel** (secteur de la construction mécanique).

2

... modifie l'usage prévu d'une machine ou étend ses fonctions. Il peut s'agir de l'**exploitant** d'une installation industrielle ou d'un **équipementier** chargé de moderniser une installation existante.

3

... importe une machine d'un pays tiers et s'engage ainsi à respecter impérativement les obligations définies par la directive à l'intention du fabricant. Il s'agit en général d'un **importateur**.

Le fabricant au sens des textes normatifs n'est pas uniquement celui qui fabrique la machine (constructeur). L'exploitant, l'équipementier ou encore l'ensemblier industriel chargé de mettre à niveau une machine (ou un parc de machines) sont également considérés comme des fabricants dès lors qu'ils modifient la machine ou en étendent les fonctions.

L'ajout de fonctionnalités supplémentaires à une machine ou l'augmentation de sa cadence de production par rapport à celle initialement prévue peuvent par ex. entraîner de nouveaux risques qui doivent être pris en compte. L'importateur qui livre des machines d'Asie en Europe par exemple, est également considéré comme fabricant en termes de responsabilité légale et doit donc veiller à ce que la machine soit conforme aux législations nationales.

1.3. Présentation des directives en vigueur

Directives CE

Elles sont adoptées par la Communauté européenne et doivent être transposées par les États membres dans la législation nationale. CE est un véritable passeport technique (obligatoire pour l'exportation au sein de l'Union européenne).

Exemples de directives importantes

- Directive Machines
- Directive Basse tension
- Directive CEM
- Directive Equipements sous pression
- Directive Jouets
- etc.

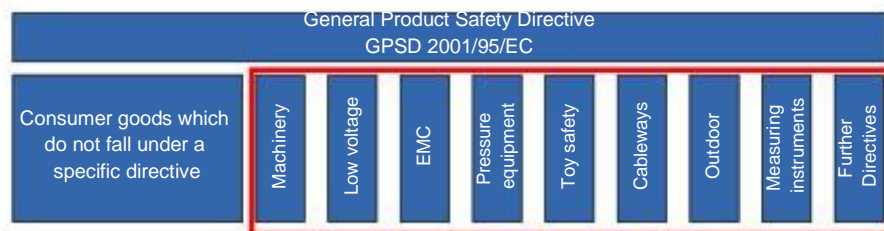
CE

Symbole de la libre circulation au sein de l'Union européenne ; ancienne abréviation de Communauté Européenne, Comunidad Europea, Comunidade Europeia et Comunità Europea.

1.4. Choix de la ou des directives

Une directive s'applique à un certain produit lorsque...

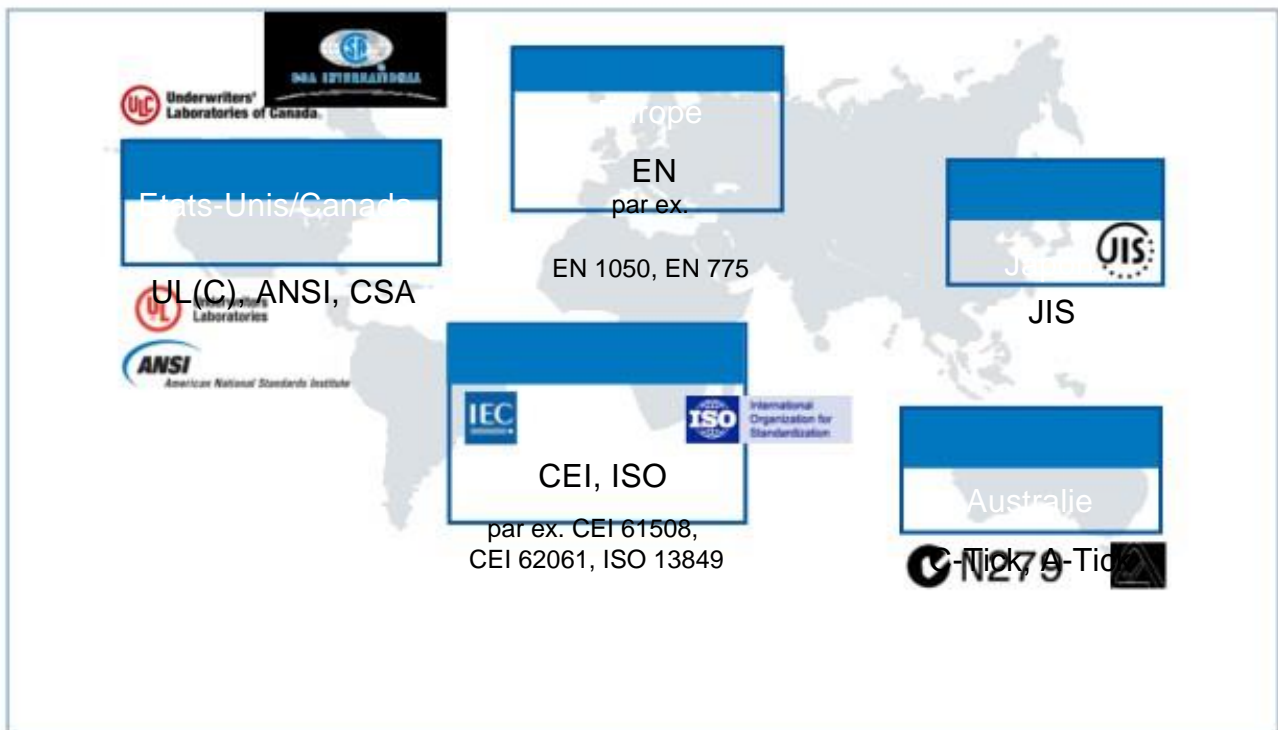
- le produit s'inscrit formellement dans le domaine d'application de cette directive ;
- le produit présente des risques décrits dans les exigences essentielles de cette directive ;
- le fait de savoir sous quelle directive une norme produit est référencée en tant que norme harmonisée donne des indications sur l'affectation à une directive ;
- les réglementations sectorielles spécifiques prévalent sur les réglementations générales.



Les directives reposent sur un concept global :

- Grâce aux directives CE, la libre circulation des marchandises est garantie au sein de l'Espace économique européen. L'objectif est de réduire tous les obstacles techniques et commerciaux qui découlent de la diversité des exigences techniques des États membres relatives aux produits techniques et à leur utilisation.
- Les directives CE ne contiennent que des objectifs de sécurité généraux et définissent les exigences essentielles en matière de sécurité.
- Les détails techniques peuvent être définis dans des normes par les organismes de normalisation mandatés par la Commission européenne (CEN, CENELEC). Ces normes, qui doivent être appliquées de la même manière par tous les États membres comme des normes nationales, figurent dans le Journal officiel de la CE et sont harmonisées sous une directive particulière.
- Certaines normes ne sont pas obligatoires. Le respect des normes harmonisées confère toutefois une « présomption de conformité » aux exigences essentielles de la directive correspondante.

1.5. Normes de sécurité internationales



■ Il convient de respecter les normes et prescriptions en vigueur sur le lieu d'implantation de la machine ou de l'installation.

UL

Underwriters Laboratories : organisme de certification pour la sécurité des produits aux États-Unis et au Canada

ANSI

American National Standards Institute : organisme américain pour la normalisation des procédés industriels

CSA

Canadian Standards Association (Association canadienne de normalisation en français) : délivre une marque de contrôle produit qui atteste de la conformité aux normes ISO, ANSI, ULC

CEI

Commission Electrotechnique Internationale (International Electrotechnical Commission - IEC en anglais) : organisme de normalisation international chargé des domaines de l'électrotechnique et de l'électronique. Certaines de ses normes sont développées conjointement avec l'ISO. Son siège est à Genève.

ISO

Organisation internationale de normalisation (International Organization for Standardization en anglais) : association internationale d'organismes de normalisation

EN

Normes européennes

JIS

Japanese Industrial Standard : norme industrielle japonaise (comparable à NF ou DIN)

C-Tick

Marquage de l'ACA (Australian Communications Authority), plus ou moins comparable au marquage CE

A-Tick

Marquage attestant la conformité aux Australian Telecommunication Standards, comparable à la directive CEM

CEN

Comité européen de normalisation, Bruxelles

CENELEC

Comité européen de normalisation électrotechnique, Bruxelles (→ EN = Normes européennes)

AFNOR

Association française de normalisation, La Plaine Saint-Denis

DIN

Deutsches Institut für Normung e.V. (institut allemand de normalisation), Berlin

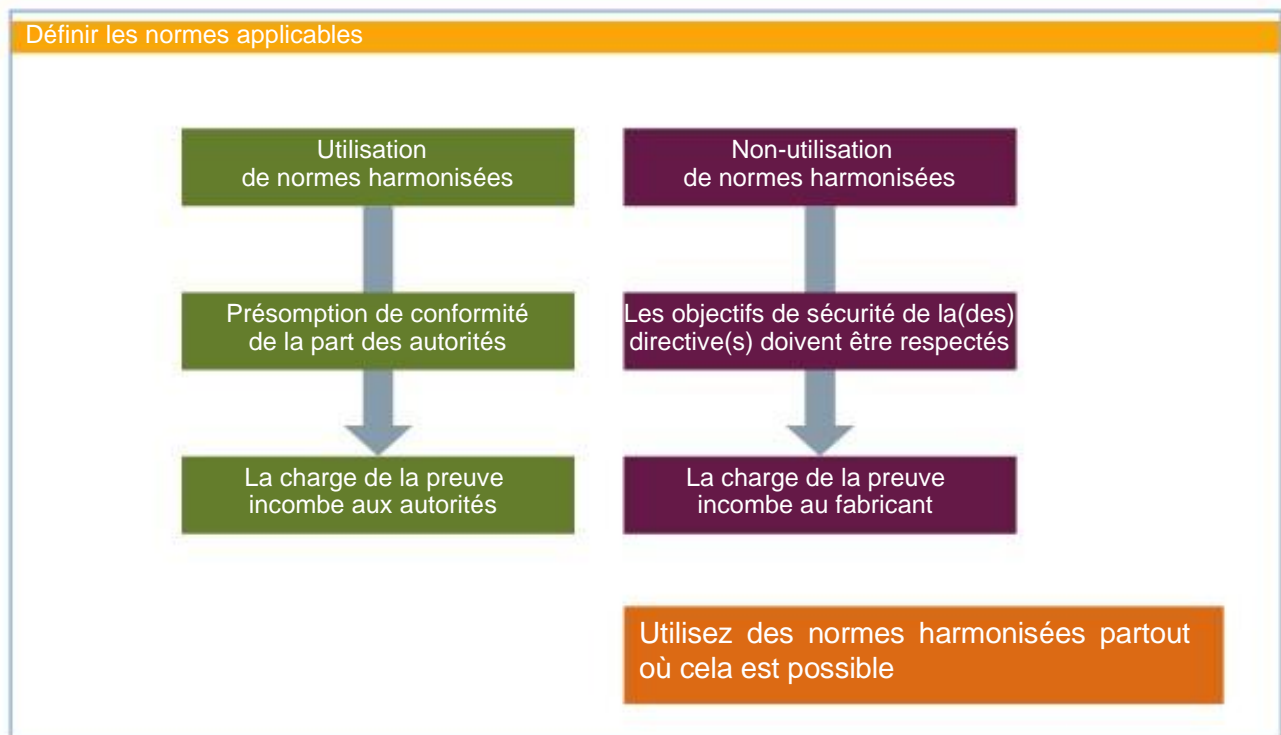
VDE

Verband der Elektrotechnik, Elektronik und Informationstechnik e.V. (fédération allemande des industries de l'électrotechnique, de l'électronique et de l'ingénierie de l'information), Francfort-sur-le-Main

Exemples de normes :

- NF EN ISO 13849-1 (norme française homologuée transposant une norme européenne transposant elle-même une norme internationale ISO)
- DIN EN ISO 13849-1 (idem pour la norme allemande)

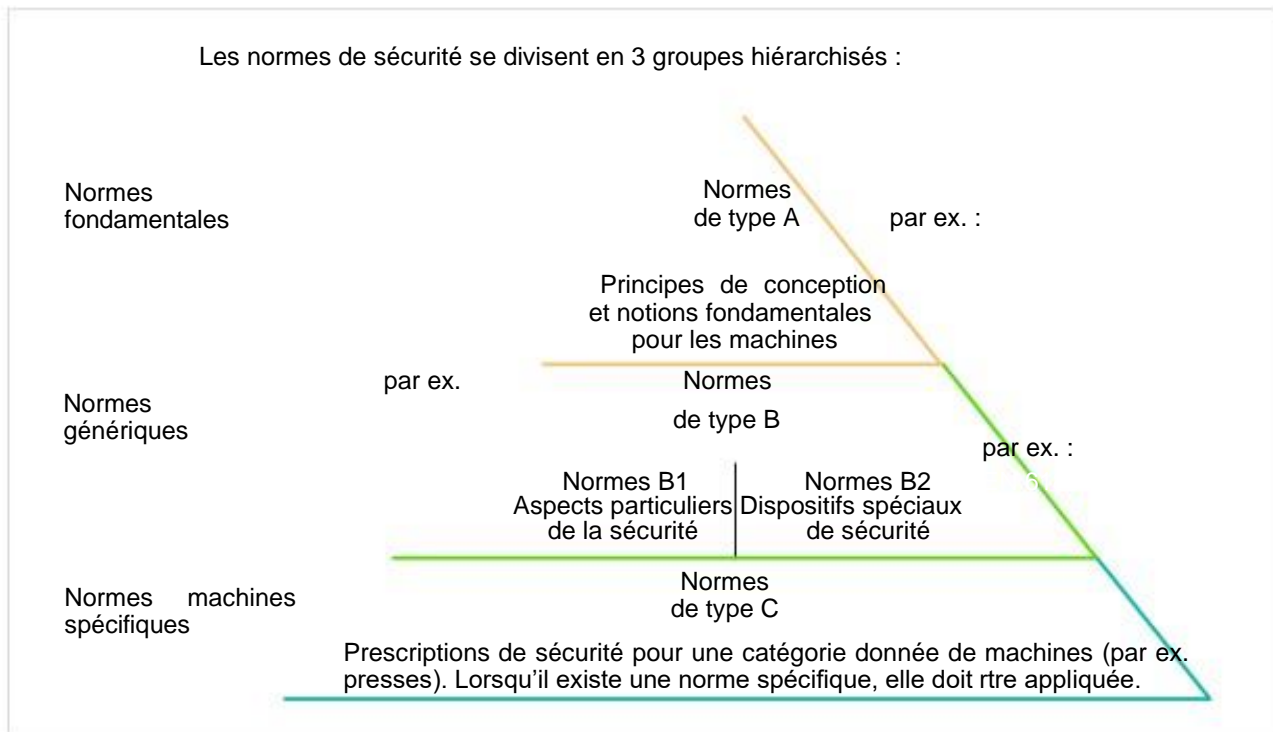
1.5.1. Normes harmonisées



Normes harmonisées

- Leur application est une démarche volontaire.
- Elles sont publiées au Journal officiel de l'Union européenne sous la référence d'au moins une directive.
- Elles sont reprises sans modifications en tant que normes nationales par tous les États membres.
- Elles reflètent l'état le plus récent de la technique.
- Elles définissent des modalités concrètes pour la mise en œuvre des objectifs de sécurité formulés par les directives.
- Elles simplifient les procédures pour prouver la conformité.
- Elles ont un domaine de validité bien défini décrivant l'utilisation et l'environnement prévus.

1.5.2. La hiérarchie des normes de sécurité



Normes fondamentales de sécurité / Normes de type A

Les normes fondamentales s'appliquent à toutes les machines. Elles fixent le cadre essentiel pour les normes B et C. Elles ne sont prises en compte par le fabricant qu'en l'absence de normes B/C. Elles définissent les notions fondamentales, les principes de conception et les aspects généraux applicables aux machines.

Normes génériques de sécurité / Normes de type B

Elles traitent d'un aspect de la sécurité ou d'un moyen de protection valable pour une large gamme de machines. Elles se répartissent en deux catégories :

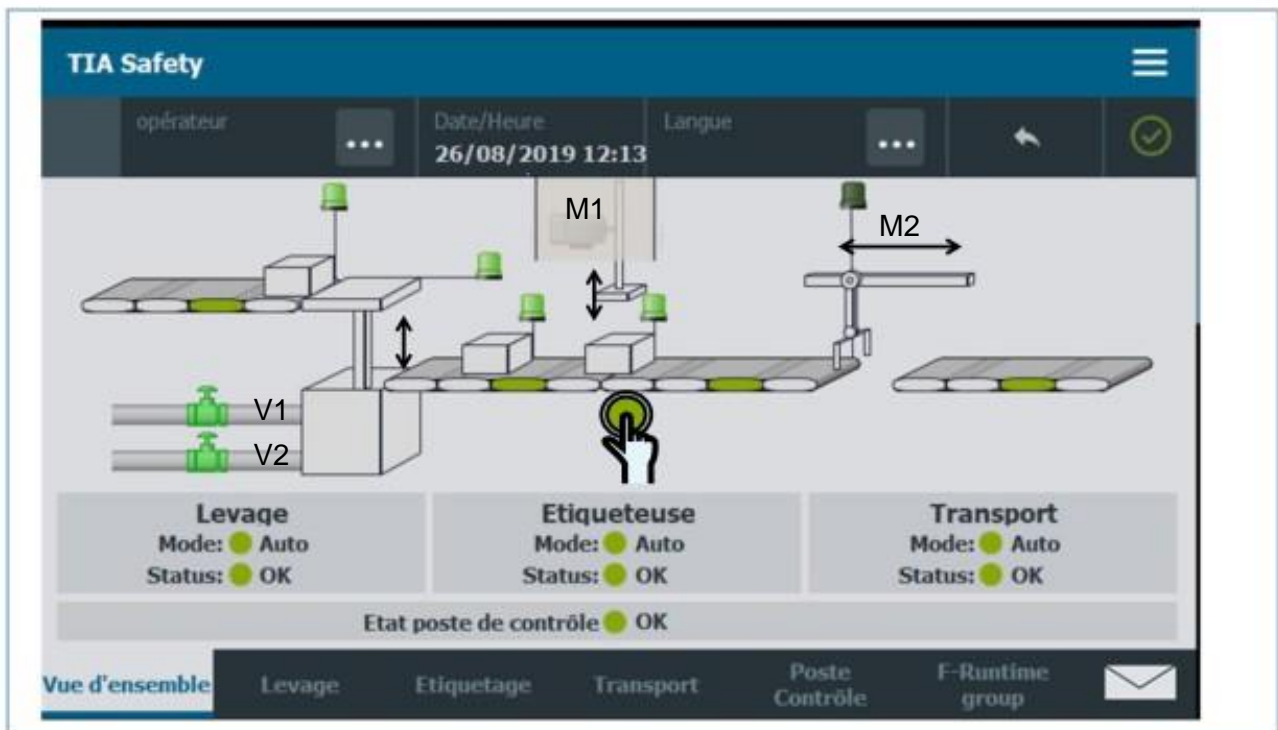
Normes de type B1 : traitent d'aspects particuliers de la sécurité (par ex. principes ergonomiques, distances de sécurité, bruit, température de surface...) ; non spécifiques aux appareils.

Normes de type B2 : traitent des moyens de protection (par ex. arrêts d'urgence, commandes bimanuelles, dispositifs de protection...) ; spécifiques aux appareils.

Normes de sécurité par catégorie de machines / Normes de type C

Elles traitent des exigences de sécurité détaillées s'appliquant à une machine particulière ou à un groupe de machines particulier (par ex. machines-outils, machines pour le travail du bois...) couvrent les exigences spécifiques d'une machine pouvant s'écarter des spécifications des normes A et B, elles ont la plus haute priorité pour le fabricant de la machine.

1.6. Exemple de machine « Étiqueteuse »



Exemple de machine « Étiqueteuse »

La machine étiquette des pièces à l'aide d'une presse à vis (M1). Les pièces sont amenées via un dispositif de levage hydraulique (V1 & V2). Une fois étiquetée, la pièce est évacuée à l'aide d'un robot de préhension (M2). Le processus d'étiquetage est surveillé à partir d'un poste de commande. Chaque étape du processus (alimentation, étiquetage et évacuation) dispose d'un mode de fonctionnement propre qui peut être piloté séparément.

Alimentation:

- Automatique
- Stop

Étiqueteuse :

- Automatique
- Stop

Évacuation :

- Automatique
- Stop
- Maintenance (Mode réglage)

Poste de commande :

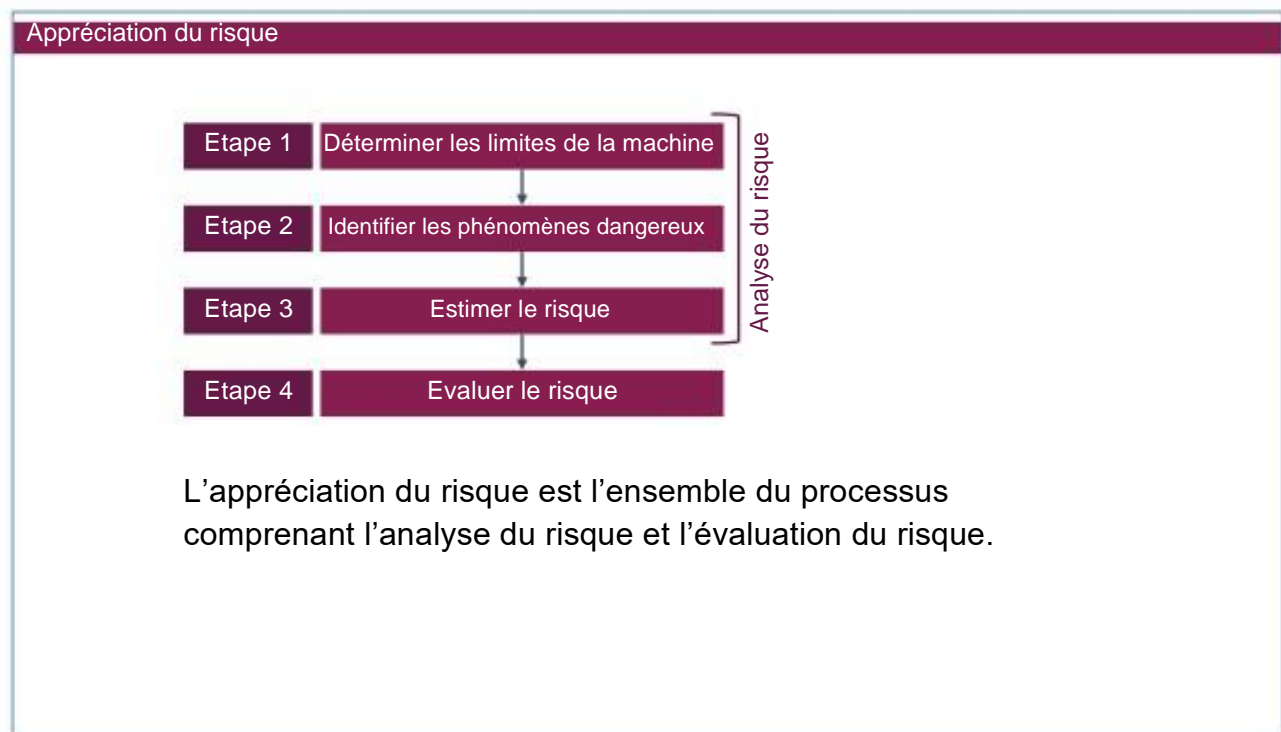
- Automatique (tous les sous-systèmes)
- Stop (tous les sous-systèmes)

1.7. Mise en œuvre de la directive Machines ± Application à une étiqueteuse

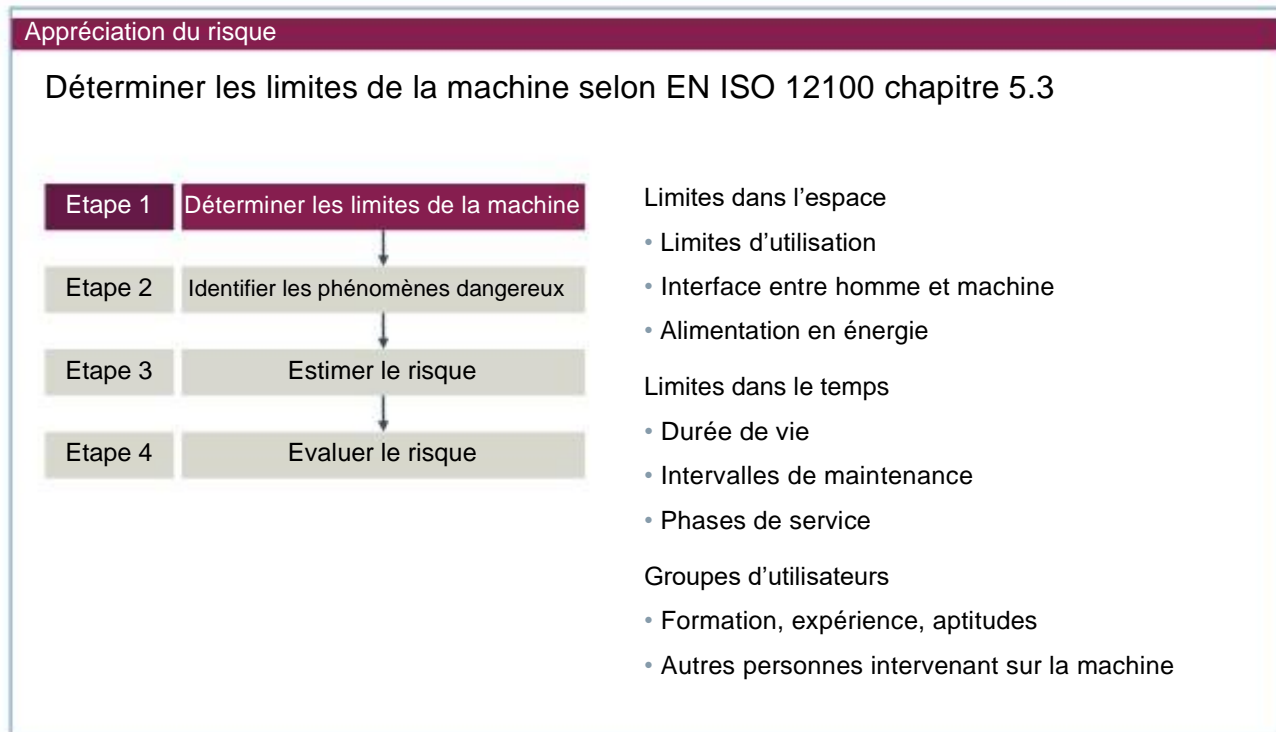
Les étapes nécessaires pour concevoir une machine sûre peuvent être représentées sous la forme d'une chaîne de processus.



1.8. Processus d'appréciation du risque selon EN ISO 12100



1.8.1. Étape 1 : Déterminer les limites de la machine



Limites dans l'espace

- Caractéristiques comme les dimensions et la masse de la machine.
- Postes de travail prévus et espaces de déplacement.
- Interfaces homme machine.
- Interfaces d'alimentation en énergie.
- Interfaces avec les machines en amont et en aval si la machine est conçue pour être exploitée en association avec d'autres machines.

Limites dans le temps

- Durée de vie prévue.
- Nombre total de rotations.
- Nombre de cycles de manœuvres.
- Opérations de remplissage et de déchargement.
- Cycles de travail ou heures de fonctionnement, etc.

Remarque :

Ces indications sont nécessaires pour la détermination des mesures et des intervalles de vérification, de maintenance et d'entretien.

1.8.1.1. Limites de la machine « Étiqueteuse »

Appréciation du risque

Extrait du descriptif de la machine (exemple) :

Usage prévu

- Machine destinée à l'étiquetage de paquets de 500 x 500 mm max. et 10 kg max.
- Alimentation en pièces via un dispositif de levage hydraulique
- Evacuation via un rail horizontal

Limites d'utilisation

- Raccordement : 400 V 3~ 50 Hz
- Installation à l'intérieur (IP54)
- Plage de température : -15 à +50°
- Étiqueteuse : 50 Nm max.
- Dispositif de levage : 10 kg max.
- Robot : rayon d'action 2 x 2 m

Groupes d'utilisateurs

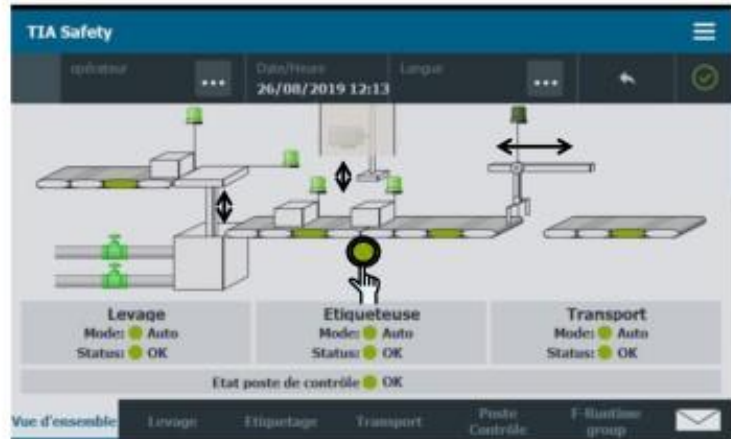
- Personnel qualifié uniquement, pas de non-professionnels
- Apprentis uniquement sous la surveillance de personnes qualifiées

Limites dans le temps

150 000 heures de fonctionnement

Limites dans l'espace

- Les aides au chargement ne font pas partie de la machine
- Place nécessaire aux personnes travaillant sur la machine



Limites d'utilisation

- Usage approprié
- Mauvais usage raisonnablement prévisible
- Caractéristiques et quantités de matières premières, consommables ou pièces
- Paramètres de fonctionnement tels que pression, température, vitesse, puissance, etc.
- Domaines d'utilisation prévus ou prévisibles (industriels, domestique, etc.)
- Conditions environnementales

Groupes d'utilisateurs

- Utilisateurs non professionnels
- Opérateurs
- Personnel de maintenance
- Régleurs

Remarque :

Un certain niveau de qualification ne peut en aucun cas justifier une éventuelle réduction du niveau de sécurité technique.

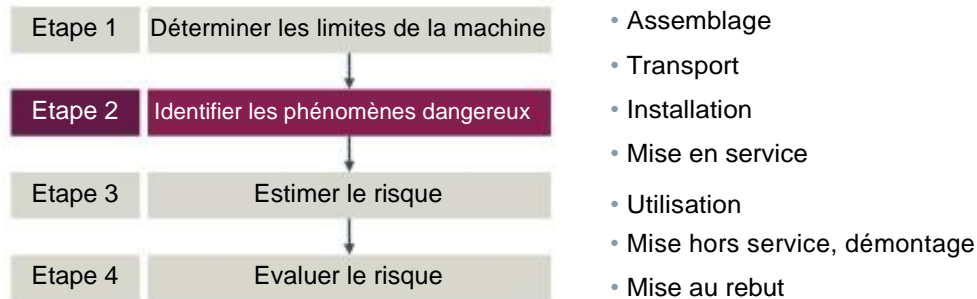
Note :

Il n'est pas possible de déterminer toutes les limites de la machine dès la première appréciation. La question de la durée de vie prévisible des pièces liées à la sécurité, par exemple, ne peut être posée que lorsque les mesures liées à leur mise en œuvre ont été déterminées. Les limites de la machine doivent être indiquées dans la notice d'instructions. Pour éviter un mauvais usage prévisible, il est recommandé d'utiliser des formulations d'exclusion lorsqu'aucune mesure de prévention technique ne peut être prise.

1.8.2. Étape 2 : Identifier les phénomènes dangereux

Appréciation du risque

Identification systématique des situations et/ou phénomènes dangereux durant toutes les phases du cycle de vie et dans tous les modes de fonctionnement de la machine :



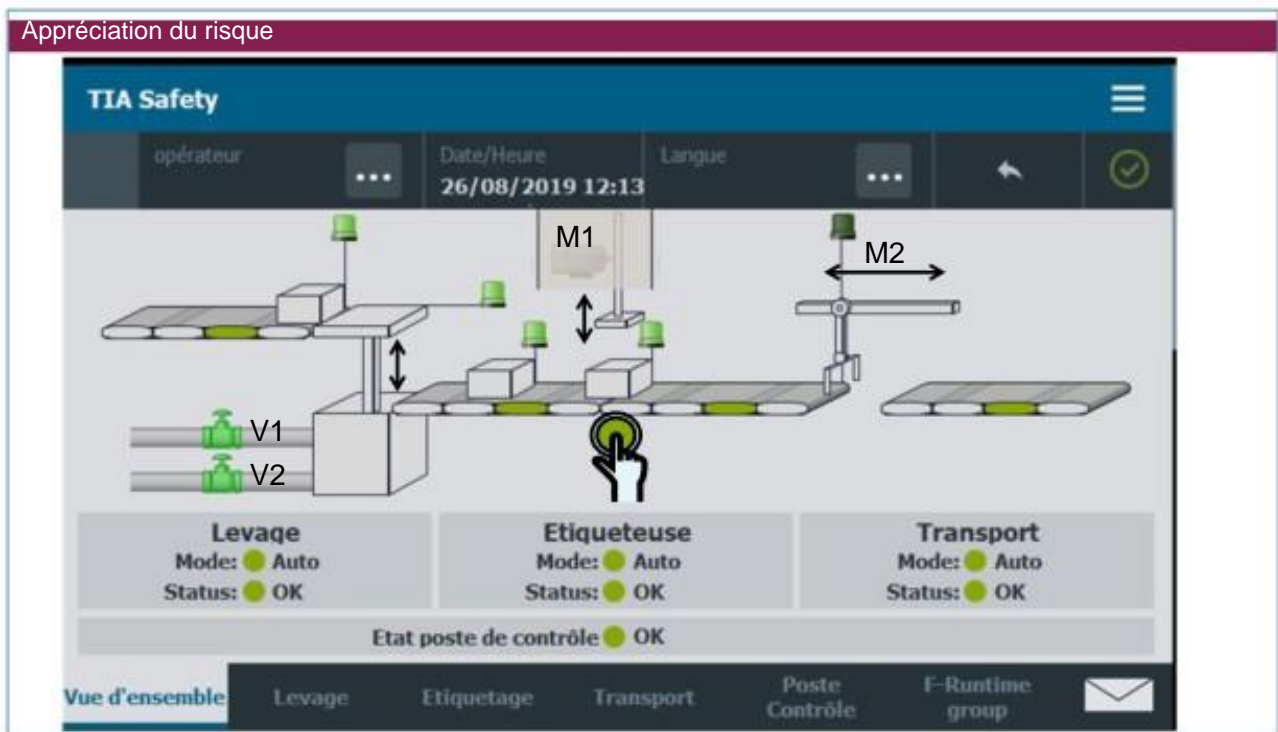
Identifiez systématiquement tous les dangers raisonnablement prévisibles à toutes les phases du cycle de vie et dans tous les modes de fonctionnement de la machine.

1.8.2.1. Phénomènes dangereux possibles

Appréciation du risque					
Phénomènes dangereux possibles selon EN ISO 12100					
Coupure	Chute	Mouvement	Force de gravité	Rapprochement	Rotation
 <ul style="list-style-type: none"> • Coupure • Sectionnement 	 <ul style="list-style-type: none"> • Ecrasement • Choc 	 <ul style="list-style-type: none"> • Ecrasement • Choc • Cisaillement 	 <ul style="list-style-type: none"> • Ecrasement • Choc • Compression 	 <ul style="list-style-type: none"> • Ecrasement • Choc 	 <ul style="list-style-type: none"> • Entraînement • Frottement • Abrasion • Ecrasement

Lors de l'identification des phénomènes dangereux possibles, vous devez toujours considérer les différentes phases du cycle de vie de la machine et ses différents modes de fonctionnement. Exemple : lors de la phase Fabrication en série, les phénomènes dangereux peuvent être différents dans les modes Manuel et Automatique, car la machine est exploitée à des vitesses différentes en fonction du mode de fonctionnement.

1.8.2.2. Exercice 1 : Identifier les phénomènes dangereux sur la machine



Enoncé

Identifier les phénomènes dangereux de l'étiqueteuse pour les modes de fonctionnement automatique et maintenance.

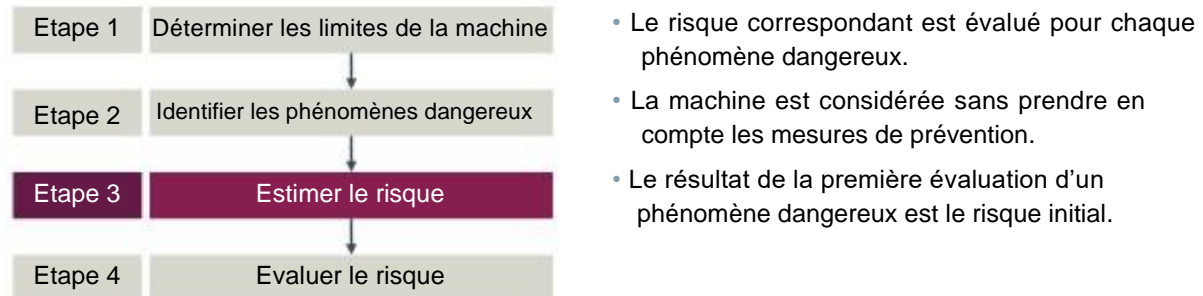
Réalisation

Discuter des phénomènes dangereux en groupe, notez-les (iPad/bloc-notes). Puis partager vos résultats lors d'une discussion commune.

1.8.3. Étape 3 : Estimer le risque

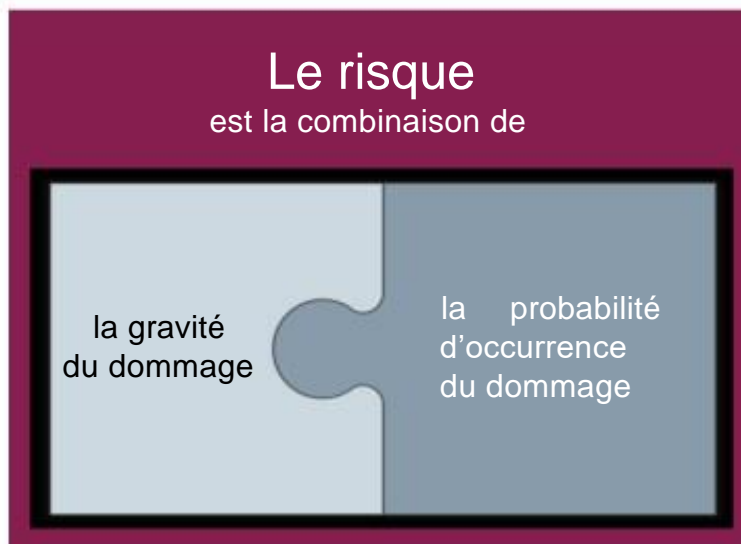
Appréciation du risque

Evaluation approfondie de la probabilité d'occurrence et de la gravité d'un dommage résultant des phénomènes dangereux déterminés :




1.8.3.1. Risque

Appréciation du risque

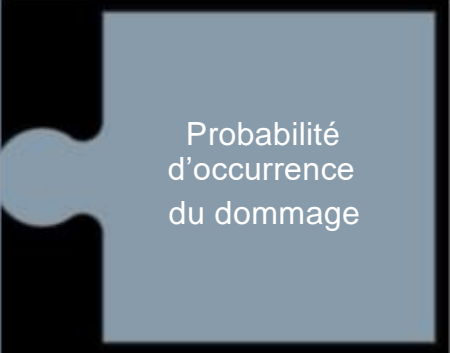


1.8.3.2. Gravité du dommage

Appréciation du risque	
	<p>Gravité du dommage pouvant résulter du phénomène dangereux</p> <ul style="list-style-type: none">• Réversible, premiers soins• Réversible, traitement médical nécessaire• Membres fracturés, perte de doigts• Irréversible, mort, perte d'un œil ou d'un bras

Lors de l'évaluation de la gravité du dommage, vous devez établir une distinction fondamentale entre dommages réversibles et dommages irréversibles.

1.8.3.3. Probabilité d'occurrence du dommage

Appréciation du risque	
 <p>Probabilité d'occurrence du dommage</p>	<p>Fréquence et durée d'exposition au phénomène dangereux</p> <ul style="list-style-type: none"> • Besoin d'accès à la zone dangereuse • Nature de l'accès et durée d'exposition • Nombre de personnes, fréquence d'accès <p>Probabilité d'occurrence du phénomène dangereux</p> <ul style="list-style-type: none"> • faible • moyenne • forte <p>Possibilité d'éviter le phénomène dangereux ou de limiter le dommage</p> <ul style="list-style-type: none"> • Rapidité d'apparition : soudaine, rapide ou lente • Qualification des personnes • Conscience du risque • Action réflexe, expérience pratique • Agilité, possibilité de fuite

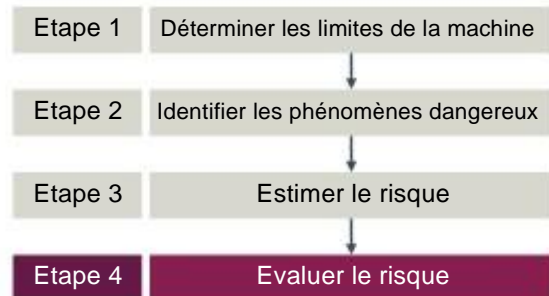
Trois facteurs influencent considérablement la probabilité d'occurrence d'un dommage :

- La fréquence et la durée d'exposition au phénomène dangereux
- La probabilité d'occurrence du phénomène dangereux
- La possibilité d'éviter le phénomène dangereux ou de limiter le dommage

1.8.4. Étape 4 : Évaluer le risque

Appréciation du risque

La question centrale est la suivante : le risque (initial) engendré par chaque zone dangereuse est-il acceptable ou faut-il prendre des mesures ?



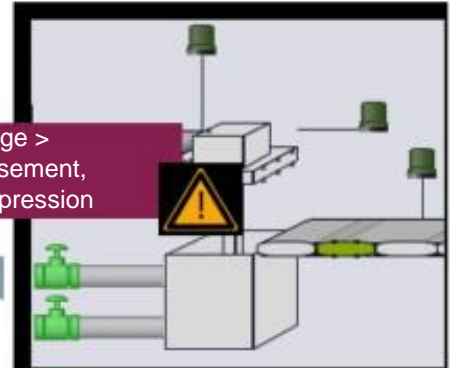
1.8.4.1. Exercice 2 : Évaluer le risque (dispositif de levage)

Evaluation du risque

Sévérité	Probabilité d'occurrence

Gravité du dommage	Probabilité d'occurrence			
	A Très probable	B Probable	C Improbable	D Très improbable
4 Irréversible : - Mort - Perte d'un œil - Perte d'un bras				
3 Membre fracturé - Perte de doigts				
2 Réversible : - Traitement médical				
1 Réversible : - Premiers soins				

Levage >
Ecrasement,
Compression



Enoncé

Réaliser l'évaluation du risque pour le phénomène dangereux suivant :
Pincement ou écrasement du bras ou de la main par le dispositif de levage

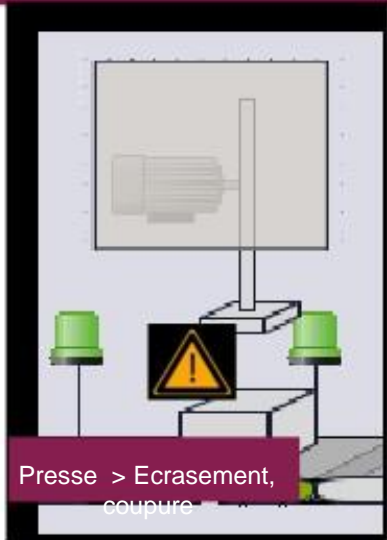
Mise en œuvre

Réaliser l'évaluation de l'ampleur du dommage au niveau de votre groupe (cf. exercice 1) à l'aide du graphe des risques. Reporter cette évaluation au niveau du graphe.

1.8.4.2. Exercice 3 : Évaluer le risque (tampon pour étiquetage)

Evaluation du risque

Sévérité		Probabilité d'occurrence			
		A	B	C	D
Gravité du dommage		Très probable	Probable	Improbable	Très improbable
4 Irréversible : - Mort - Perte d'un œil - Perte d'un bras					
3 Irreversible : - Membre s fracturés - Perte de doigts					
2 Réversible : - Traitement médical					
1 Réversible : - Premiers soins					



Presse > Ecrasement, coupure

Enoncé

Réaliser l'évaluation du risque pour le phénomène dangereux suivant :
Pincement ou sectionnement de la main ou du doigt par le tampon d'étiquetage

Mise en œuvre

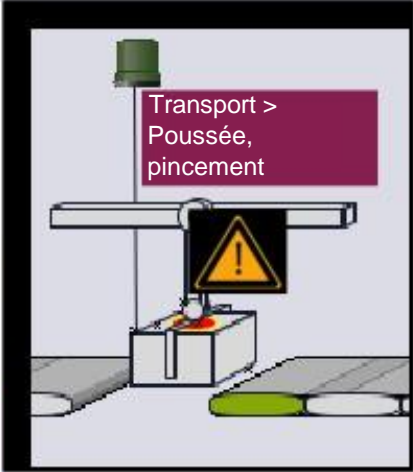
Réaliser l'évaluation de l'ampleur du dommage au niveau de votre groupe (cf. exercice 1) à l'aide du graphe des risques. Reporter cette évaluation au niveau du graphe.

1.8.4.3. Exercice 4 : Évaluer le risque (Robot d'évacuation)

évaluation du risque

Sévérité		Probabilité d'occurrence			

Gravité du dommage		Probabilité d'occurrence			
		A Très probable	B Probable	C Improbable	D Très improbable
4	Irréversible : - Mort - Perte d'un œil - Perte d'un bras				
	3	Membre s fracturés - Perte de doigts			
2	Réversible : - Traitement médical				
1	Réversible : - Premiers soins				



Transport > Poussée, pincement

Enoncé

Réaliser l'évaluation du risque pour le phénomène dangereux suivant :
Poussée ou pincement de la tête ou du torse lors du déchargement par évacuation

Mise en œuvre

Réaliser l'évaluation de l'ampleur du dommage au niveau de votre groupe (cf. exercice 1) à l'aide du graphe des risques. Reporter cette évaluation au niveau du graphe.

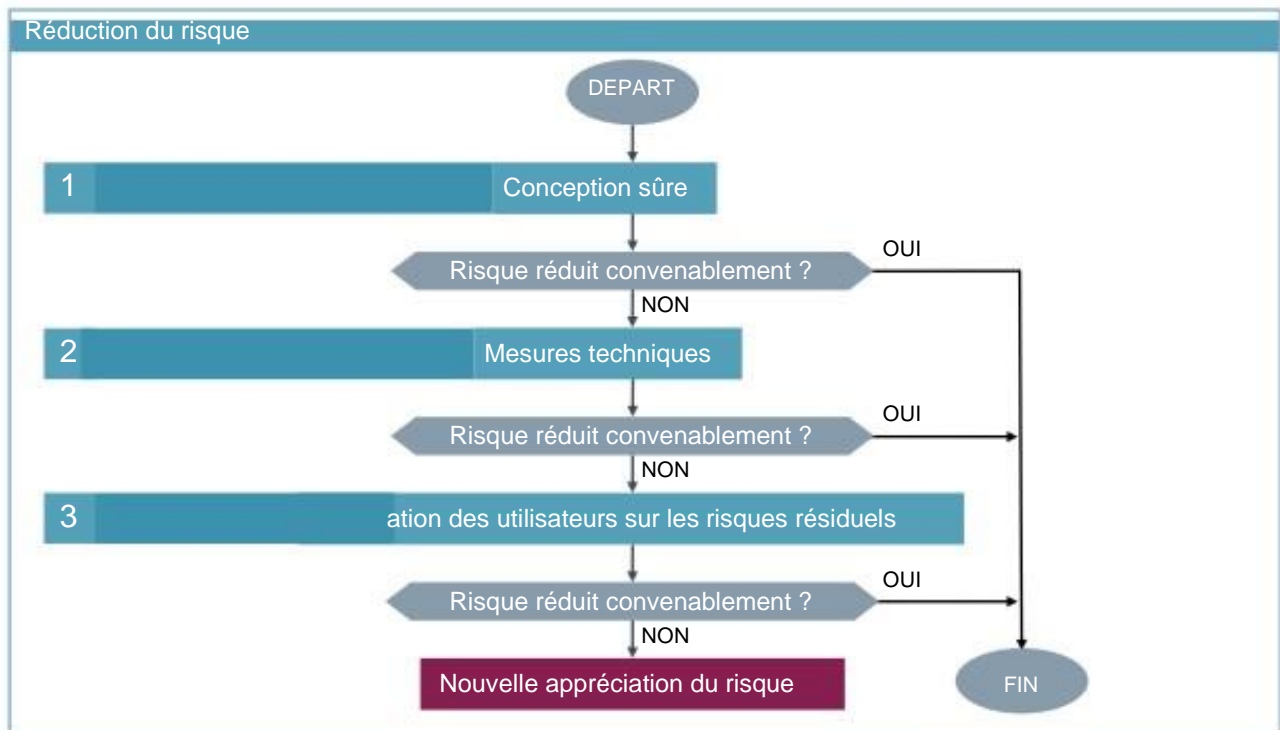
1.8.5. Résumé

Appréciation du risque

- La machine et les risques qu'elle engendre ont été décrits et évalués.
- Le résultat de l'appréciation du risque constitue le fondement du concept de sécurité pour la réduction du risque.
- Une appréciation correcte du risque permet de contester tout reproche de négligence en cas de dommage.

Le risque établi pour la machine de l'exemple vous permet de définir une valeur de risque dans le graphique de risques. En mettant en œuvre les mesures appropriées, vous pourrez déplacer le risque de la zone rouge vers la zone verte optimale.

1.9. Réduction du risque selon EN ISO 12100



Pour définir et évaluer les mesures de sécurité, utilisez la méthode à trois étapes décrite par la norme harmonisée EN ISO 12100. Cette méthode peut être visualisée à l'aide d'un graphe de décision.

Commencez toujours par définir des mesures de sécurité constructives. Si ces mesures conduisent déjà à un risque résiduel acceptable, aucune autre mesure n'est nécessaire. Ces mesures purement constructives peuvent toutefois être contournées par le personnel d'exploitation et ne pas conduire à elles seules à un risque résiduel acceptable. Des mesures de sécurité techniques complémentaires s'imposent alors.

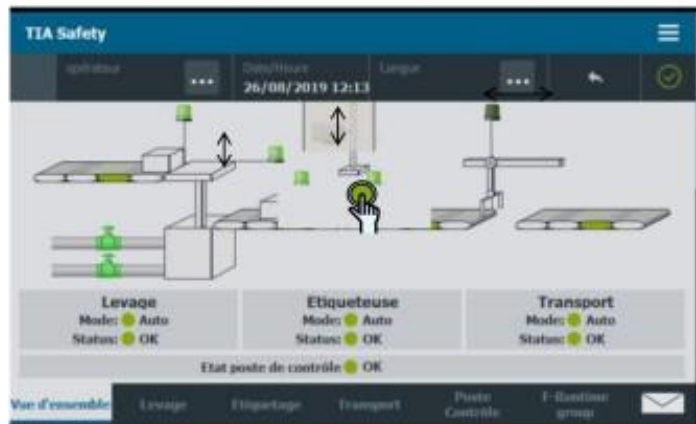
Si des risques demeurent après la mise en œuvre de mesures de sécurité techniques, ils peuvent généralement être réduits par une information des utilisateurs et des instructions d'utilisation. Exemples : port de vêtements de protection, respect de distances de sécurité, opérations à effectuer dans un ordre prescrit, etc.

1.9.1. Étape 1 : Conception sûre

Réduction du risque

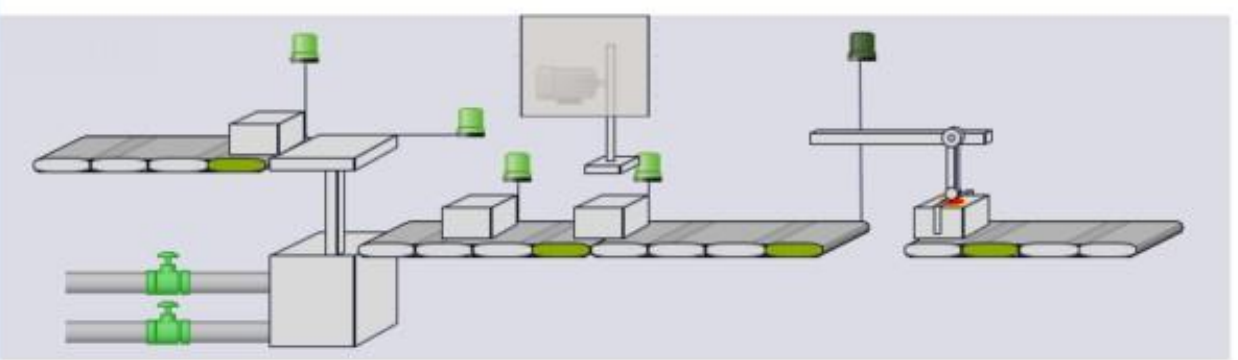
La conception sûre de la machine est la priorité la plus importante lors de la réduction des risques !

- Intégration de la sécurité dès la conception de la machine
- Exploitation et maintenance sûre par mesures constructives
- Possibilité évidente de réduction de la gravité du dommage
- Les informations relatives à une construction sûre se trouvent sous EN ISO 12100 Para. 6.2



1.9.1.1. Exercice 5 : Mesures pour une conception sûre

Réduction du risque



Gravité du dommage	A Très probable	B Probable	C Improbable	D Très improbable
4 Irréversible : - Mort - Perte d'un œil - Perte d'un bras	4A (Transport)			
3 Irréversible : - Membres fracturés - Perte de doigts	3A (Etiqueteuse)	3B (Dispositif de levage)		

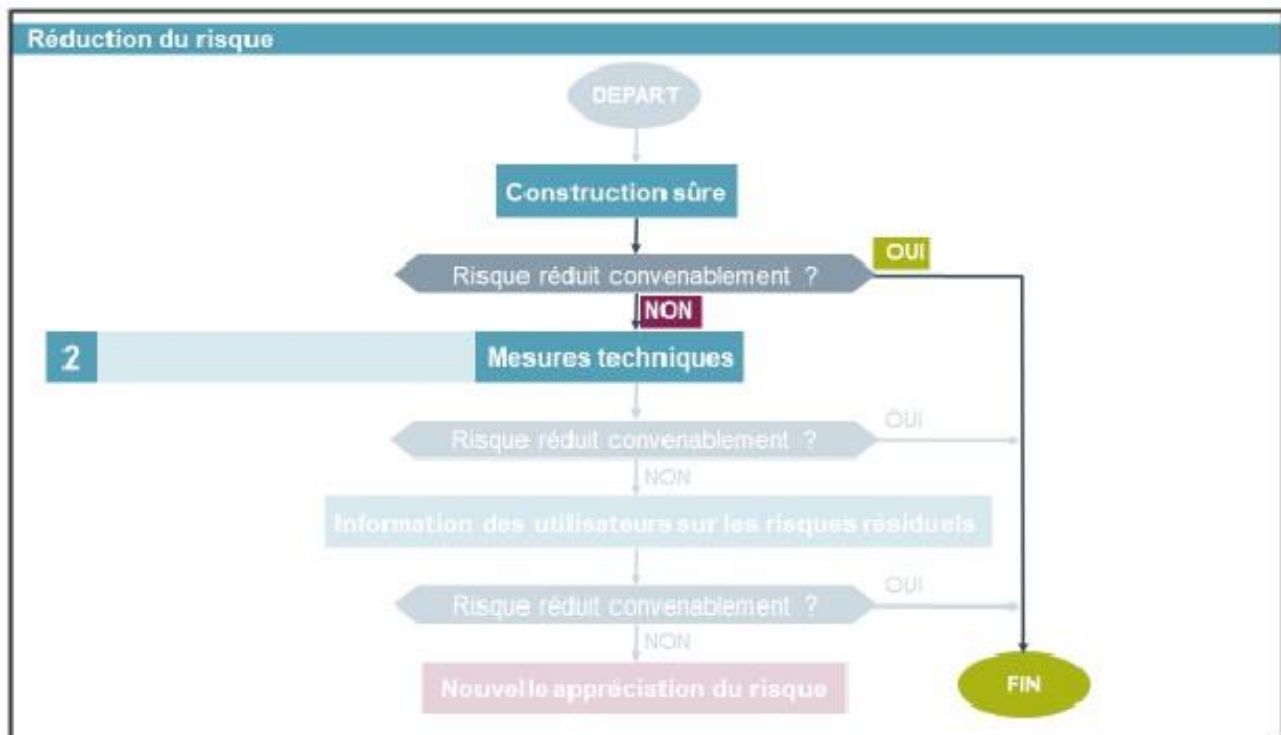
Enoncé

Trouver les mesures constructives adéquates.

Mise en œuvre

Réaliser la discussion en groupe et noter les mesures (iPad ou bloc-notes). Discuter les mesures et réaliser la synthèse commune.

1.9.2. Étape 2 : Mesures de protection techniques



Si la conception de la machine est sûre, aucune autre mesure n'est nécessaire selon la méthode à trois étapes.

Dans notre exemple toutefois, la conception n'offre pas encore une sécurité suffisante. Des mesures techniques supplémentaires doivent donc être mises en œuvre.

Exemple:

- Barrière immatérielle pour surveiller les personnes qui s'approchent de la zone dangereuse.
- Tapis de sécurité pour localisation des personnes.
- Interrupteur de sécurité avec verrouillage électromagnétique surveillé.
- Commande bimanuelle et à pédale.
- Les commutateurs d'assentiment autorisent l'accès sous certaines conditions qui représentent un risque moins important.
- Mesure de sécurité complémentaires, par ex. arrêt d'urgence

1.9.2.1. Exercice 6 : Mesures de protection techniques possibles



Enoncé

Trouver les mesures de protection techniques adéquates.

Mise en œuvre

Réaliser la discussion en groupe et noter les mesures (iPad ou bloc-notes). Discuter les mesures et réaliser la synthèse commune.

1.9.2.2. Exercice 7 : Évaluation des mesures techniques

Réduction du risque

Evaluation des mesures techniques

Gravité du dommage		Probabilité d'occurrence			
		A Très probable	B Probable	C Improbable	D Très improbable
4	Irréversible : - Mort - Perte d'un œil - Perte d'un bras			4C (Transport)	
3	Irréversible : - Membres fracturés - Perte de doigts	3A (Etiqueteuse)			
2	Réversible : Traitement médical				
1	Réversible : Premiers soins				

Risques résiduels actuels : _____

1.9.2.3. L'architecture des fonctions de sécurité définissent les gradations du risque par des Niveaux de sécurité

Réduction du risque

Les niveaux de sécurité définissent la qualité des mesures techniques de protection

- L'importance du risque détermine le niveau de sécurité requis
- La définition du risque et des niveaux de sécurité correspondants varient d'une norme à l'autre

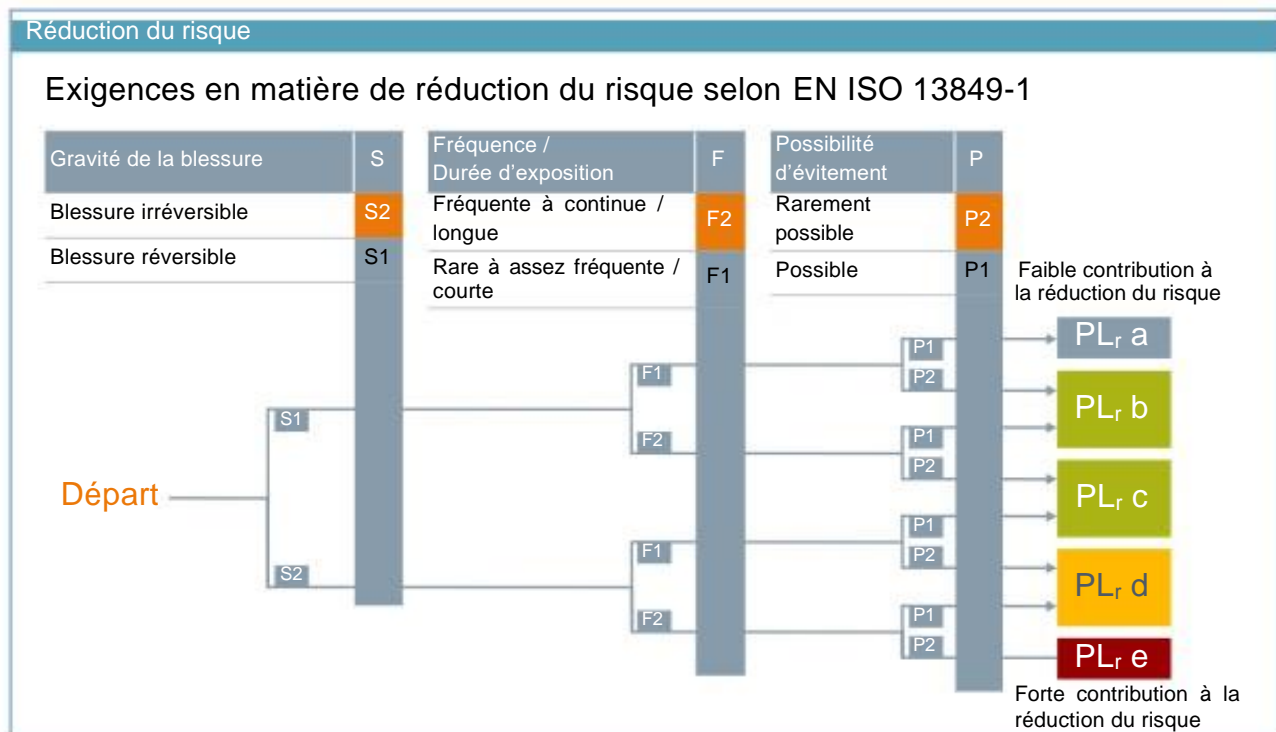
En matière de sécurité fonctionnelle (sécurité des machines), il existe 2 normes qui définissent des niveaux de sécurité différents

- EN ISO 13849-1 Niveau de performance PL a à PL e
- CEI 62061 Niveau d'intégrité de sécurité SIL 1 à SIL 3

Niveaux de sécurité selon l'importance du risque

Le niveau de sécurité doit être défini en fonction de l'importance du risque. Pour ce faire, deux normes différentes peuvent être appliquées.

1.9.2.4. Exigences selon EN ISO 13849-1



Réduction du PL sur la base d'une probabilité d'occurrence réduite du phénomène dangereux (par. A.2.3.2)

L'annexe A a fait l'objet de nombreuses modifications.

Elle commence par souligner de manière plus explicite le caractère informatif de la procédure de détermination du PL_r décrite dans l'Annexe A : celle-ci n'est pas obligatoire et ne représente qu'une évaluation de la réduction du risque. Les normes de type C peuvent tout à fait s'écarter, dans leurs définitions du PL_r, du PL_r qui pourrait résulter du graphe de risques en raison des compromis normatifs définis par les groupes d'experts compte tenu du fait que certaines causes peuvent ne pas être couvertes par les paramètres du graphe de risques.

La remarque concernant la distinction entre F1 et F2 est désormais formulée comme suit :


- En l'absence d'autre justification, F2 doit être choisi lorsque la fréquence est supérieure à une fois toutes les 15 minutes.
- F1 peut être choisi lorsque la durée d'exposition totale n'excède pas 1/20 de la durée totale de service et que la fréquence n'est pas supérieure à une fois toutes les 15 minutes.

A cela s'ajoute désormais la probabilité d'apparition d'un événement dangereux. Lorsqu'elle est évaluée comme faible, le PL_r peut être réduit d'un niveau. Une réduction supplémentaire du PL_r a n'est pas prévue.

1.9.2.6. Signification des niveaux de sécurité

Réduction du risque

Les niveaux de sécurité SIL ou PL déterminent le niveau de fiabilité requis d'un système de sécurité :

Niveau de sécurité SIL	PL	Fiabilité requise du système de sécurité (en défaillances/heure)	Mesures d'amélioration de la fiabilité
-	PL a	10^{-5} à 10^{-4}	 Utilisation de « composants éprouvés » Essais de fonctionnement réguliers Détection automatique des défaillances Conception redondante Redondance + détection de défauts
SIL 1	PL b	3×10^{-6} à 10^{-5}	
SIL 1	PL c	10^{-6} à 3×10^{-6}	
SIL 2	PL d	10^{-7} à 10^{-6}	
SIL 3	PL e	10^{-8} à 10^{-7}	

En cas de mise en œuvre correcte d'un système de sécurité, sa probabilité de défaillance équivaut à la probabilité d'apparition d'un phénomène dangereux. Les normes EN 62061 et EN ISO 13849-1 définissent ainsi un risque quantitatif et vont donc plus loin que la norme EN 954-1.

Les deux évaluations donnent un résultat indiquant un taux de défaillance qui permet d'établir clairement le niveau de risque encouru. Le niveau de probabilité d'apparition d'un danger peut ainsi être défini.

Ce taux peut être calculé selon les deux normes à partir des paramètres spécifiques aux appareils. Il permet d'indiquer si la mise en œuvre de la fonction de sécurité est suffisante pour atteindre le niveau de sécurité requis.

Le PL et le SIL peuvent être comparés, mais ne sont pas équivalents.

Sans mesures complémentaires, il n'est pas possible d'atteindre le niveau de certification supérieur (pour passer par ex. de SIL2 à SIL3).

Les normes EN 62061 et EN ISO 13849-1 considèrent les fonctions de sécurité comme suit :

- Une fonction de sécurité définie peut être affectée à un risque particulier (engendré par la machine)
- Le niveau de sécurité requis peut être déterminé pour une fonction de sécurité définie

Une fonction de sécurité doit être définie pour chaque danger n'ayant pas pu être éliminé au moyen de mesures constructives. Celle-ci peut être réalisée à l'aide d'un système de sécurité. Les systèmes de sécurité doivent offrir des performances correspondant au danger considéré et au risque évalué.

- EN 62061 : Niveau d'intégrité de sécurité (SIL)
- EN ISO 13849 : Niveau de performance (PL)

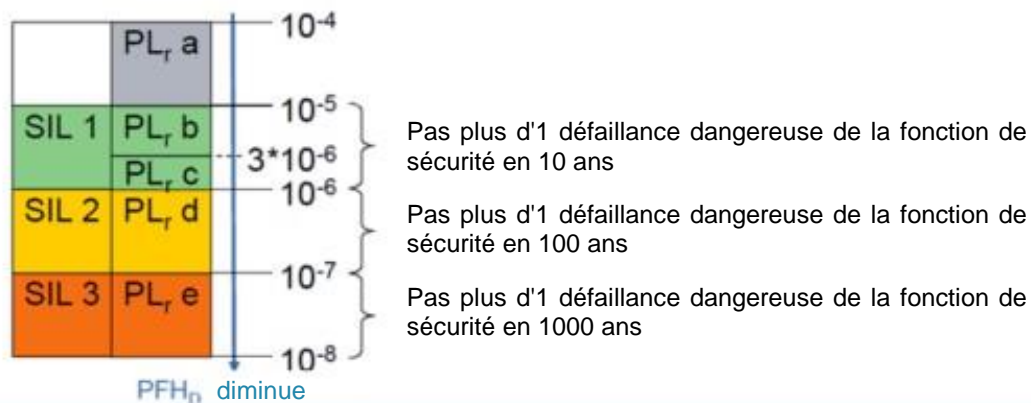
1.9.2.7. Définition du niveau de sécurité

Réduction du risque

Exigences relatives aux niveaux de sécurité : probabilité de défaillance

Les normes EN 62061 et EN ISO 13849-1 définissent les exigences en matière de probabilité de défaillance maximale admissible de la fonction de sécurité :

- Probabilité d'une défaillance dangereuse par heure PFH_D
- Plus le niveau de sécurité est élevé, plus la PFH_D doit être faible



Grandeurs statistiques

Les niveaux de sécurité calculés et atteints, qui représentent les « défaillances dangereuses pour une durée donnée », sont toujours des grandeurs statistiques. En d'autres termes, si un niveau de sécurité SIL 1 atteint par ex. une valeur de $2,7 \times 10^{-5}$, cela signifie théoriquement que 1,1826 défaillances dangereuses sont susceptibles de se produire dans les 5 ans. Cela ne veut pas dire qu'une telle défaillance aura forcément lieu après ce délai de 5 ans ; de même, on ne peut être certain que « rien ne se passera » sur une période de 4 ans.

Si une défaillance se produit, cela ne signifie pas non plus que plus aucune défaillance n'aura lieu au cours des 4 années suivantes ; il est également possible (et probable) qu'aucune défaillance ne se produise pendant 12 ans.

1.9.2.8. Une machine « sûre » - Composants de sécurité certifiés

Réduction du risque

13 L'utilisation de composants de sécurité certifiés constitue une mesure efficace pour atteindre un niveau de risque acceptable:

13 Avantages:

- 13 Perte de temps minimale pour le dimensionnement des fonctions de sécurité
- 13 Economie de coûts et d'espace
- 13 Facilitent les essais et contrôles de réception



- Les composants de sécurité doivent être testés suivants les normes appropriées.
- Les essais et contrôles de réception sont assurés par le TÜV, BG / IFA pour l'Allemagne par exemple ou par des organismes de contrôles pour la France.

Les composants de sécurité certifiés facilitent les contrôles de réception.

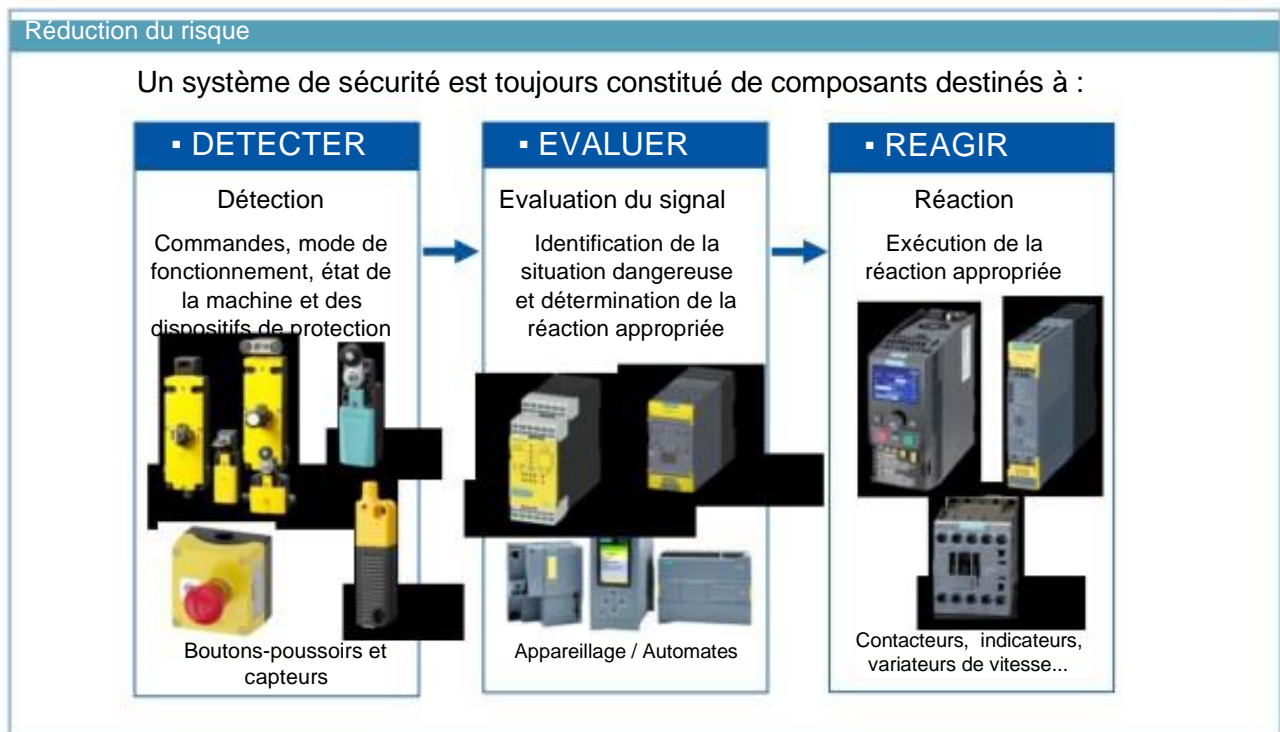
Les entraînements Siemens sont certifiés, par ex. : G120 (SIL2), S120 (SIL2, PL d)

D'autres composants de détection et de traitement (logique) disposent également de certificats. Les composants certifiés ne garantissent pas qu'un PL ou un SIL requis sera effectivement atteint. Les composants des sous-systèmes peuvent le garantir en cas de connexion appropriée. Ce n'est en revanche pas garanti avec l'interaction DETECTION-EVALUATION-REACTION. En d'autres termes, l'utilisation

- D'un capteur SIL3
- D'une logique SIL3
- D'un actionneur SIL3

Ne signifie pas que la fonction de sécurité va atteindre automatiquement le niveau SIL3.

1.9.2.9. Principe des systèmes de sécurité



Trois sous-systèmes : détection, évaluation et réaction

Détection

Elle peut être divisée en deux catégories : les systèmes de commande (poste de commande bimanuel, bouton poussoir d'assentiment...) et les appareils de commutation (interrupteurs de position, capteur optique...).

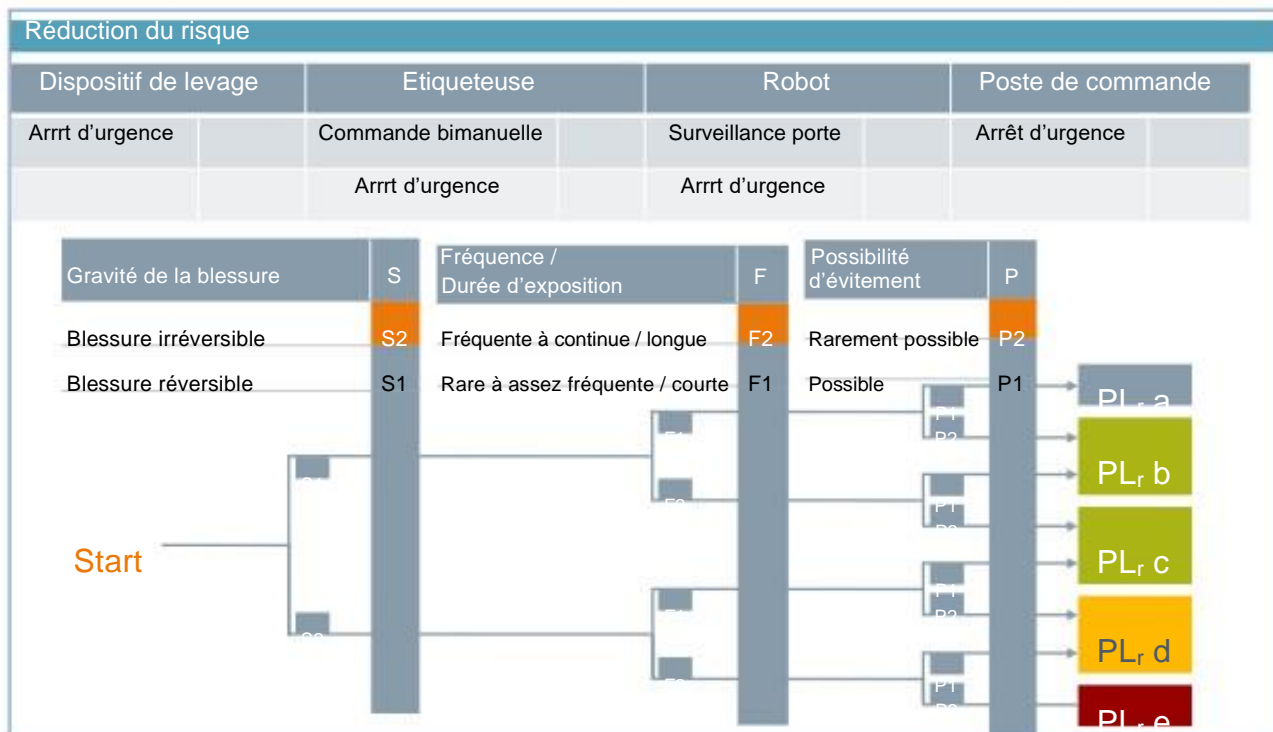
Évaluation

Rassemble les blocs logiques de sécurité (3SK) et les automates avec composants périphériques (DI, DQ, et systèmes de bus) ; c'est à ce niveau que s'opère la liaison logique entre la détection et la réaction.

Réaction

Les actionneurs arrêtent les mouvements dangereux. Il peut s'agir de contacteurs, de variateurs de vitesse, vannes etc.

1.9.2.10. Exigences auxquelles doivent répondre les fonctions de sécurité de l'étiqueteuse

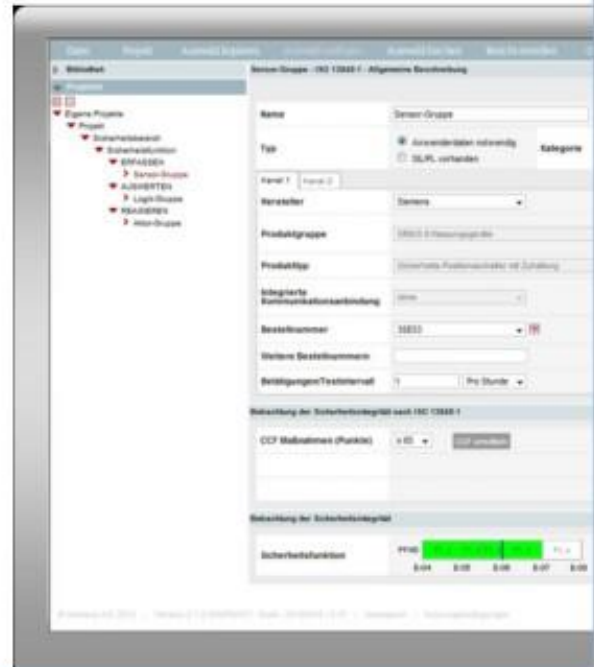


1.9.2.11. Vérification des fonctions de sécurité

Réduction du risque

La vérification des fonctions de sécurité est une obligation

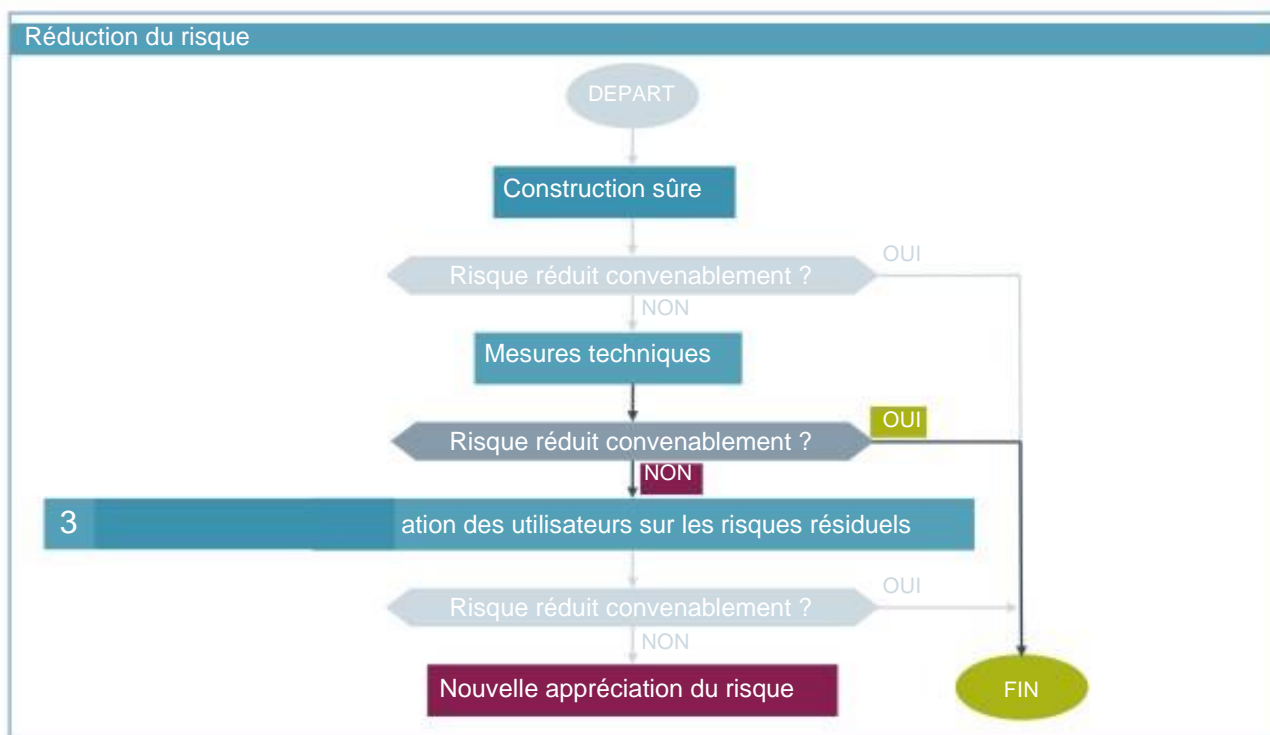
- Prescrite par les normes EN ISO 13849 et EN 62061
- Le concept de sécurité doit être évalué à l'aide d'un calcul de probabilité de défaillance et documenté
- Evaluation possible à l'aide de l'outil SET (Safety Evaluation Tool)
- Utilisation gratuite de l'outil en ligne : www.siemens.de/safety-evaluation-tool



Vos fonctions de sécurité vous permettent-elles d'atteindre le niveau de sécurité déterminé ? Le meilleur moyen de le vérifier est d'utiliser l'outil gratuit SET (Safety Evaluation Tool) de Siemens.

Pour plus d'information, voir www.siemens.de/safety-evaluation-tool.

1.9.3. Étape 3 : Information des utilisateurs sur les risques résiduels



Dans notre exemple de machine, les mesures de sécurité supplémentaires offrent suffisamment de sécurité pour rendre le risque résiduel acceptable. Vous n'avez donc aucune mesure technique supplémentaire à mettre en œuvre.

Si les mesures techniques ne permettaient pas d'atteindre un niveau de risque résiduel acceptable, il faudrait informer les utilisateurs des risques résiduels conformément à la méthode en 3 étapes.

1.9.4. Résumé

Réduction du risque

- Les mesures constructives et techniques mises en œuvre ont minimisé le risque avec une efficacité telle qu'aucune mesure technique supplémentaire n'est nécessaire.
- L'utilisation de techniques conformes à l'état de l'art actuel garantit la sécurité juridique.
- Si des risques subsistent, il est nécessaire d'informer les utilisateurs, par ex. à l'aide d'avertissements appropriés et de formations.

1.10. Attestation de conformité

Attestation de conformité

Le constructeur élabore le dossier technique attestant la conformité de sa machine. La directive Machines, Annexe VII, stipule quel doit être le contenu du dossier technique.

La documentation doit notamment comprendre :

- l'évaluation des risques
- la documentation relative au projet avec cahier des charges, plan de sécurité, plan de vérification, plan de validation
- la documentation relative au développement avec plans de contrôle et rapports d'essais
- les manuels

La documentation est essentielle pour établir les responsabilités en cas de dommages corporels.

1.10.1. Évaluation de la conformité

Attestation de conformité

Pour attester la conformité de sa machine avec les dispositions de la ou des directives applicables, le constructeur ou son mandataire réalise une procédure d'évaluation de la conformité.

Procédures possibles selon la directive Machines 2006/42/CE : ▪

Contrôle interne de la fabrication

- Examen de type
- Système d'assurance qualité

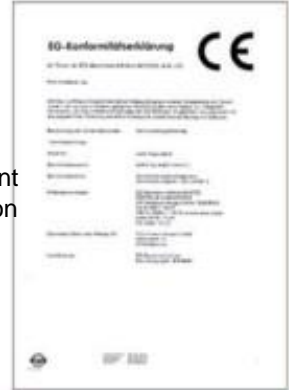
1.10.2. Contenu de la déclaration CE de conformité

Attestation de conformité

La déclaration CE de conformité pour les machines doit comprendre les éléments suivants :

- le nom et l'adresse du constructeur ou de son mandataire établi au sein de la Communauté ;
- la description de toutes les dispositions pertinentes auxquelles la machine satisfait ;
- le cas échéant, le nom et l'adresse de l'organisme notifié, ainsi que le numéro de l'attestation d'examen CE de type ;
- le cas échéant, le nom et l'adresse de l'organisme notifié auquel les documents ont été transmis (selon l'art. 12, par. 3) ;
- le cas échéant, le nom et l'adresse de l'organisme notifié ayant effectué l'examen (selon l'art. 12, par. 3) et, le cas échéant, les références aux normes harmonisées ;
- le cas échéant, les normes et spécifications techniques nationales appliquées ;
- les informations relatives au signataire habilité à signer au nom du fabricant ou de son mandataire établi au sein de la Communauté.

Dans la Déclaration d'incorporation d'une quasi-machine (machine ne pouvant fonctionner de manière indépendante mais qui constitue un élément de construction d'une autre machine ou installation), il convient en outre de déclarer les parties de machine à incorporer et de préciser que la quasi-machine ne doit pas être mise en service avant que la machine dans laquelle elle doit être incorporée ait été déclarée conforme aux dispositions de la directive.



Attestation de conformité / Contenu de la déclaration CE de conformité

Pour donner suite à la refonte de la directive Machines (2006/42/CE du 17 mai 2006), l'ancienne déclaration du fabricant doit être obligatoirement remplacée par une déclaration d'incorporation depuis le 29 décembre 2009.

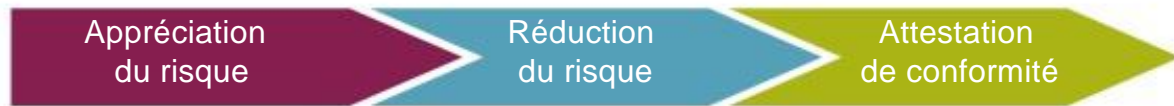
Contrairement à l'ancienne « déclaration du fabricant », la déclaration d'incorporation contient des données techniques de sécurité. La teneur de la déclaration d'incorporation est présentée à l'Annexe II 1 B de la directive Machines sous forme d'une liste de vérification.

La déclaration d'incorporation est délivrée pour une quasi-machine par le fabricant ou par son mandataire. D'après l'Annexe II B de la directive, elle doit indiquer que la mise en service d'une machine ou d'une installation dans laquelle ce composant est intégré est interdite tant que la conformité à la directive n'est pas établie. La déclaration doit également comprendre les données suivantes (en complément aux exigences de la réglementation précédemment en vigueur) :

- La raison sociale et l'adresse du constructeur ; la description du produit et des informations d'identification (désignation, fonction, modèle, type, numéro de série, dénomination commerciale) ;
- Le nom et l'adresse de la personne autorisée à constituer le dossier technique ; elle doit être domiciliée au sein de la CE ;
- Une déclaration précisant les exigences de la directive Machines qui sont appliquées, et une autre indiquant la constitution du dossier technique d'après l'Annexe VII B ;
- Une déclaration d'engagement à transmettre les documents requis sur demande dûment motivée des autorités nationales ; cette déclaration précise les modalités de transmission ;
- Les coordonnées de la personne déposant la déclaration d'incorporation.

Le marquage CE ne peut pas être apposé sur des quasi-machines selon la directive Machines.

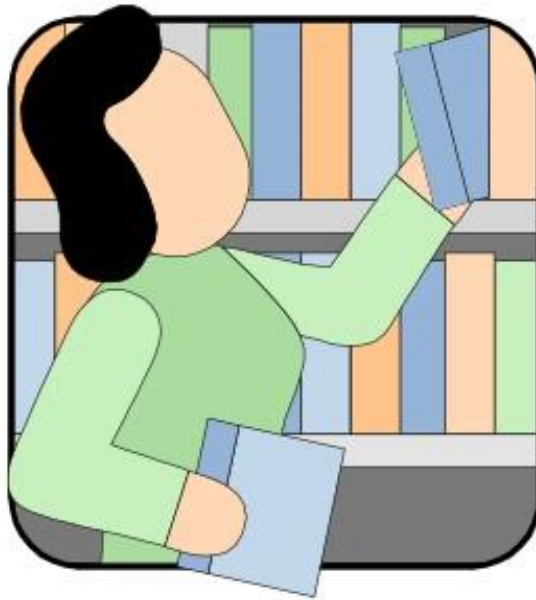
1.11. Résumé



- La directive Machines a force de loi.
- La directive Machines est obligatoire pour tous les fabricants de machines et applicable à toutes les solutions de sécurité utilisées.
- L'utilisation de normes harmonisées réduit le risque de responsabilité du fait de la présomption de conformité.
- L'utilisation de produits certifiés dans les applications selon EN 62061 et EN ISO 13849 facilitent la mise en œuvre de solutions de sécurité.

Un choix gagnant : une machine sûre, des économies, la sécurité juridique

1.12. Annexe



1.12.1. La directive européenne Machines

Directive Machines 2006/42/CE de l'Union européenne

<http://www.newapproach.org> // <http://eur-lex.europa.eu>

- Elle décrit les exigences essentielles de santé et de sécurité relatives aux machines.
- Le respect de la directive Machines 2006/42/CE est une condition préalable à l'apposition du marquage CE.
- La directive européenne Machines est transposée dans le droit national et revêt par conséquent un caractère obligatoire.



1.12.2. Formations sur les normes

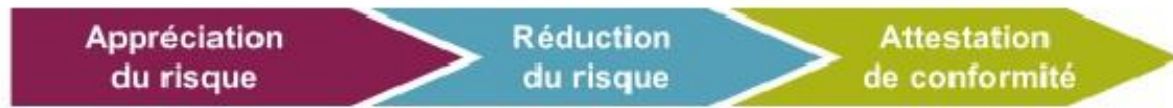
Cours dispensés par le centre de formation SITRAIN

<http://sitrain.automation.siemens.com/sitrainworld/>

ST-FASAFN

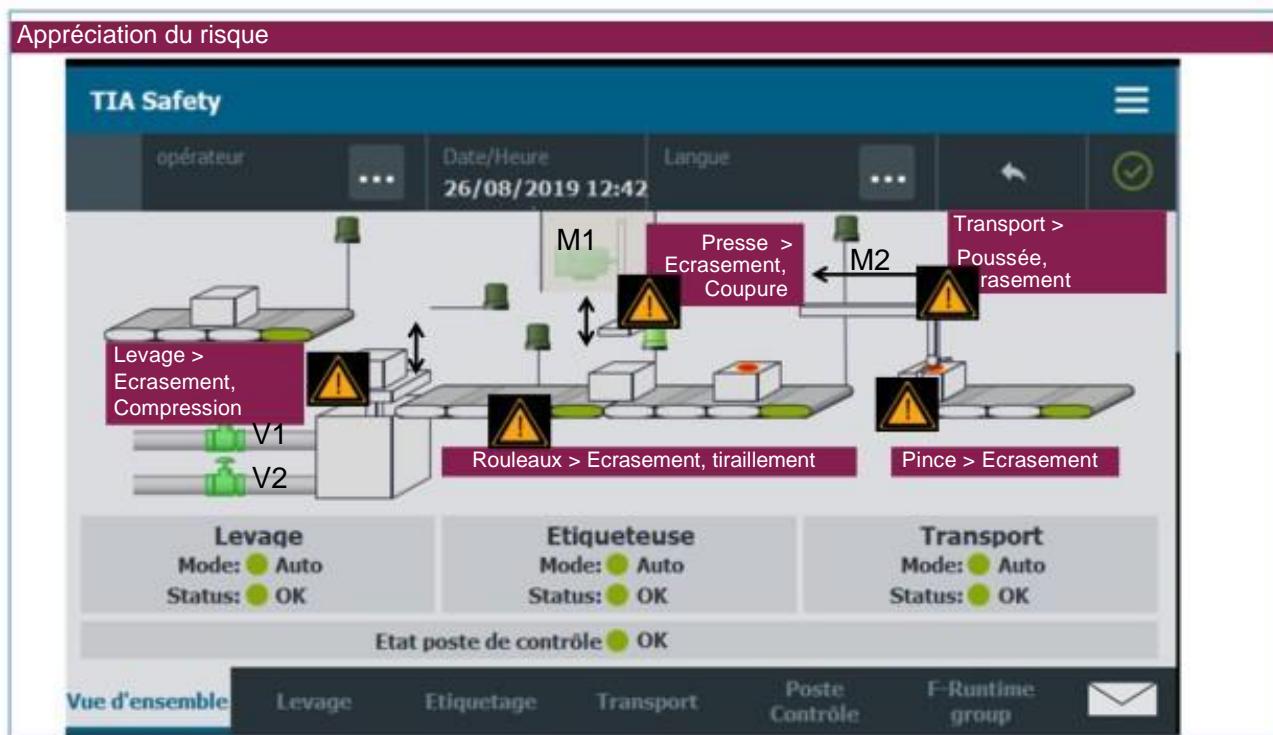
Marquage CE et sécurité fonctionnelle dans la construction de machines et d'installations

1.13. Solutions possibles aux exercices 1 à 8



Les solutions proposées ne représentent qu'une possibilité parmi d'autres et n'ont pas de caractère obligatoire. En matière d'appréciation du risque et de réduction du risque, il n'existe pas de solution « unique ».

1.13.1. Exercice 1

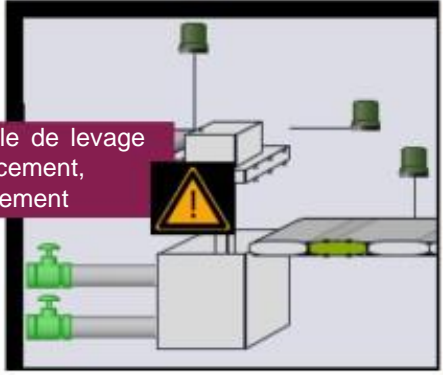


1.13.2. Exercice 2

Evaluation du risque

Sévérité
Irréversible:
- membres fracturés
- perte de doigts

Probabilité d'occurrence
Il est probable qu'une blessure se produise.



Module de levage
> Pincement, écrasement

Gravité du dommage		Probabilité d'occurrence			
		A Très probable	B Probable	C Improbable	D Très improbable
4 Irréversible : - Mort - Perte d'un œil - Perte d'un bras					
3 Membres fracturés - Perte de doigts					
2 Réversible : - Traitement médical					
1 Réversible : - Premiers soins					

3B

Evaluation du risque du groupe

1.13.3. Exercice 3

Evaluation du risque

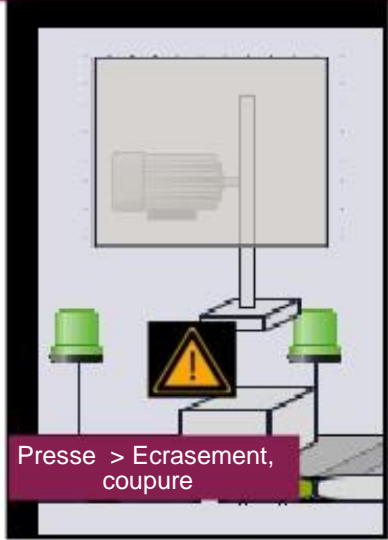
Sévérité

Irréversible:

- membres fracturés
- perte de doigts

Probabilité d'occurrence

Il est très probable qu'une blessure se produise.



Presse > Ecrasement, coupure

Gravité du dommage		Probabilité d'occurrence			
		A Très probable	B Probable	C Improbable	D Très improbable
4	Irréversible : - Mort - Perte d'un œil - Perte d'un bras	4A	4B	4C	4D
	3 Membre s fracturés - Perte de doigts	3A	3B	3C	3D
2	Réversible : Traitement médical	2A	2B	2C	2D
1	Réversible : Premiers soins	1A	1B	1C	1D

Evaluation du risque du groupe

le :

1.13.4. Exercice 4

Evaluation du risque

Sévérité

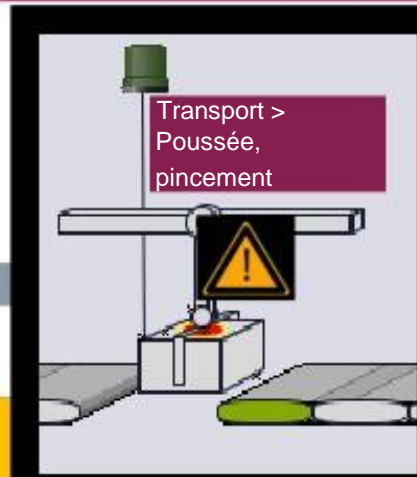
Irréversible:
- Mort
- Perte d'un œil, d'un bras

Probabilité d'occurrence

Il est très probable qu'une blessure se produise.

		Probabilité d'occurrence			
Gravité du dommage		A	B	C	D
		Très probable	Probable	Improbable	Très improbable
4	Irréversible : - Mort - Perte d'un œil - Perte d'un bras	4A			
3	Membre le : - Membre s fracturés - Perte de doigts				
2	Réversible : Traitement médical				
1	Réversible : Premiers soins				

Evaluation du risque du groupe

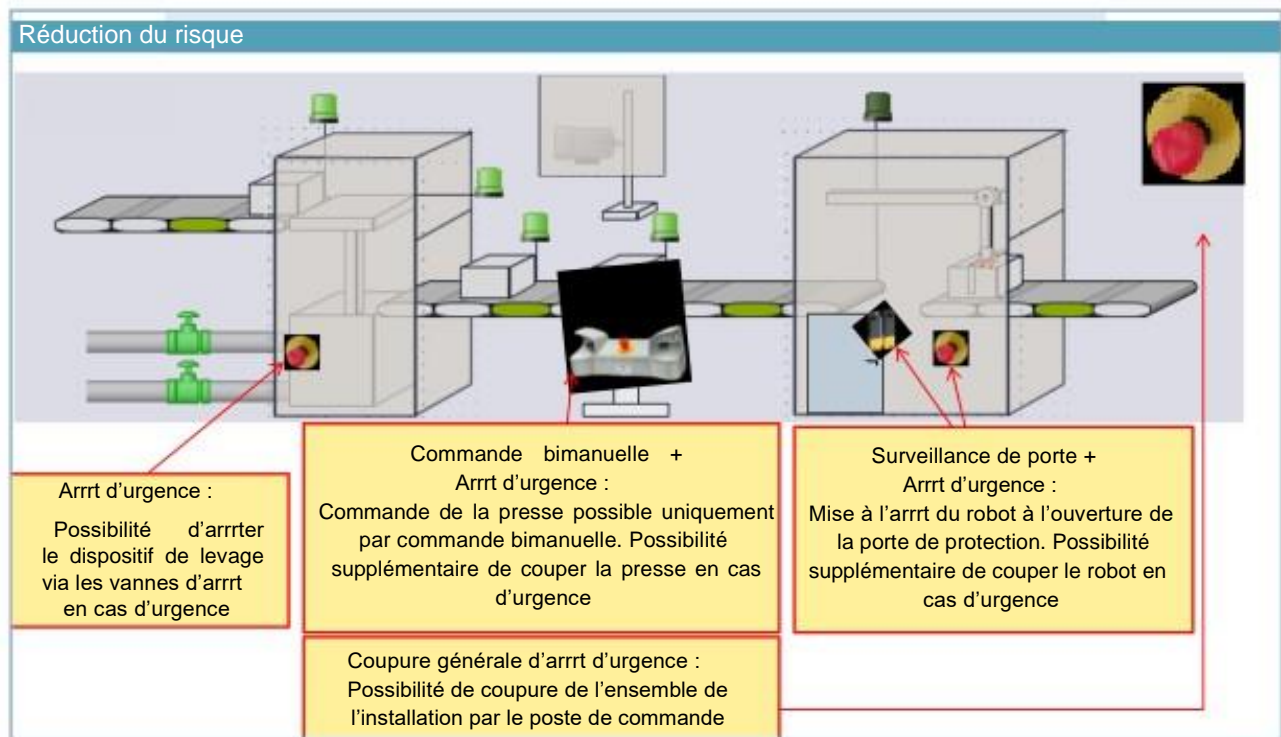


1.13.5. Exercice 5

Réduction du risque

Gravité du dommage	A Très probable	B Probable	C Improbable	D Très improbable
4 Irréversible : - Mort - Perte d'un œil - Perte d'un bras	4A (Robot)	→		
3 Irréversible : - Membres fracturés - Perte de doigts	3A (Etiqueteuse)	3B (Dispositif de levage)	→	

1.13.6. Exercice 6



1.13.7. Exercice 7

Réduction du risque

Evaluation des mesures techniques

Gravité du dommage	Probabilité d'occurrence			
	A Très probable	B Probable	C Improbable	D Très improbable
Irréversible: 4 - Mort - Perte d'un œil - Perte d'un bras			4C (Transport)	
Irréversible : 3 - Membres fracturés - Perte de doigts	3A (Etiqueteuse)			
Réversible : 2 Traitement médical				2D
Réversible : 1 Premiers soins				

Nouvelle évaluation du risque par l'équipe

Risques résiduels actuels :
D'autres mesures techniques sont-elles nécessaires ?

1.13.8. Exercice 8

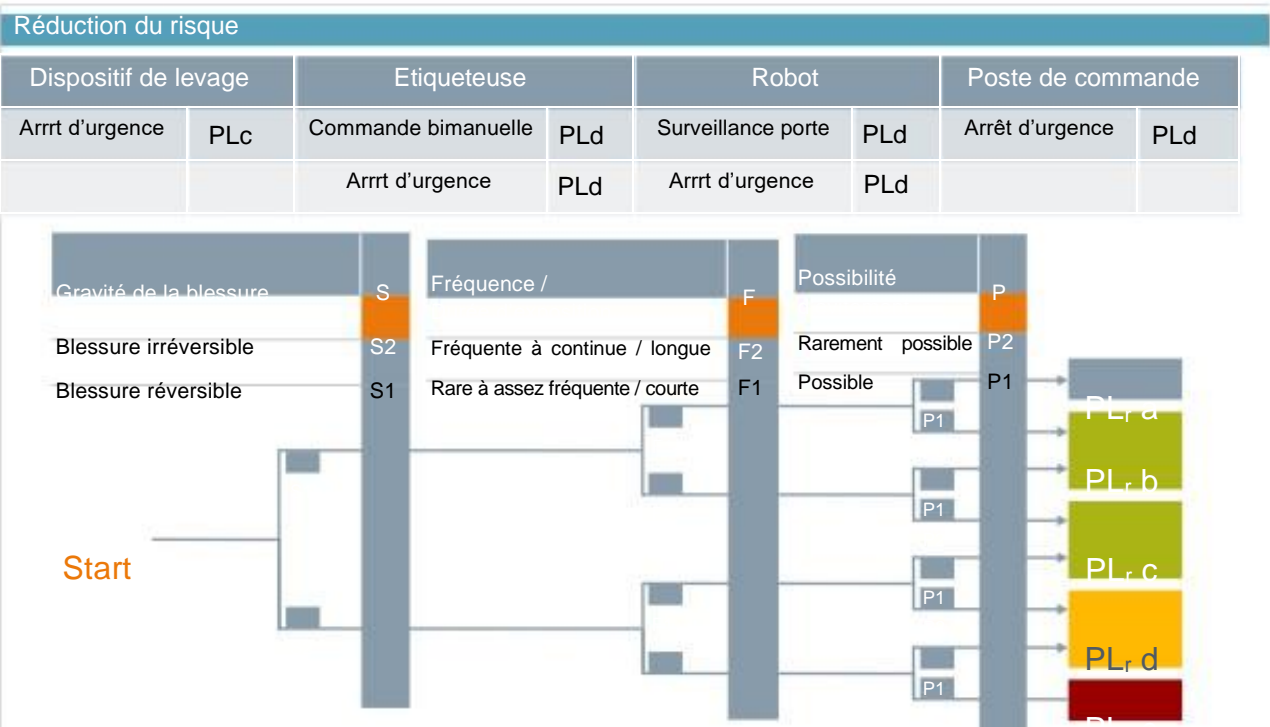


Table des matières

2.	Présentation des équipements d'automatisme	2-2
2.1.	Les contrôleurs SIMATIC	2-3
2.2.	Composantes matérielles configurables	2-4
2.3.	SIMATIC Safety Integrated : extensions	2-5
2.4.	SIMATIC Safety Integrated : configuration logicielle?	2-6
2.5.	SIMATIC S7-1200	2-7
2.5.1.	SIMATIC S7-1200	2-8
2.6.	SIMATIC S7-1500	2-9
2.7.	Périphéries de sécurité	2-10
2.8.	TIA Selection Tool	2-11
2.9.	Information complémentaire	2-13
2.9.1.	Contrôleurs ET 200SP et ET 200pro	2-14
2.9.2.	Contrôleur logiciel	2-15
2.9.3.	Contrôleur ET 200SP Open « Tout en un »	2-16
2.9.4.	SIMATIC ET 200SP	2-17
2.9.5.	Présentation des fonctions de sécurité pour SINAMICS S/G	2-18
2.9.6.	Licences disponibles	2-19

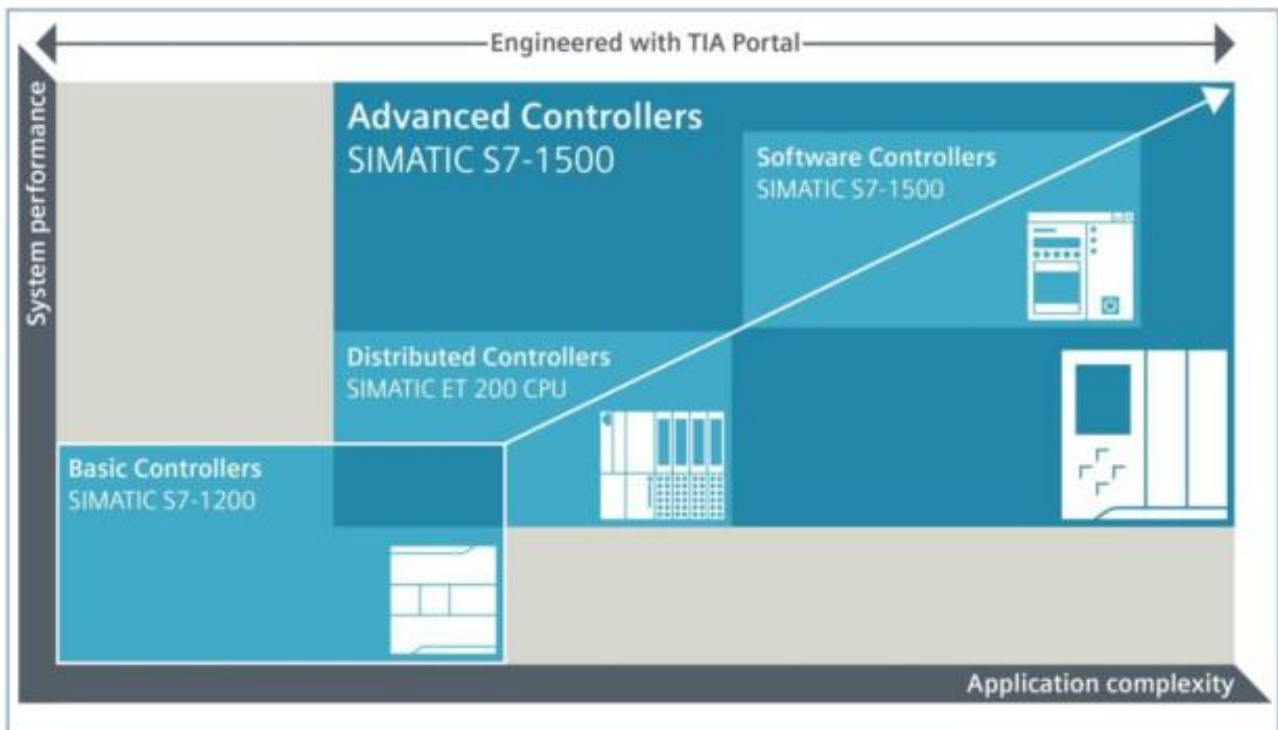
2. Présentation des équipements d'automatisme

→ l'issue de la formation, le participant au stage

... aura une vue d'ensemble sur le portefeuille des équipements
d'automatisme de sécurité disponibles sur la plateforme TIA Portal



2.1. Les contrôleurs SIMATIC

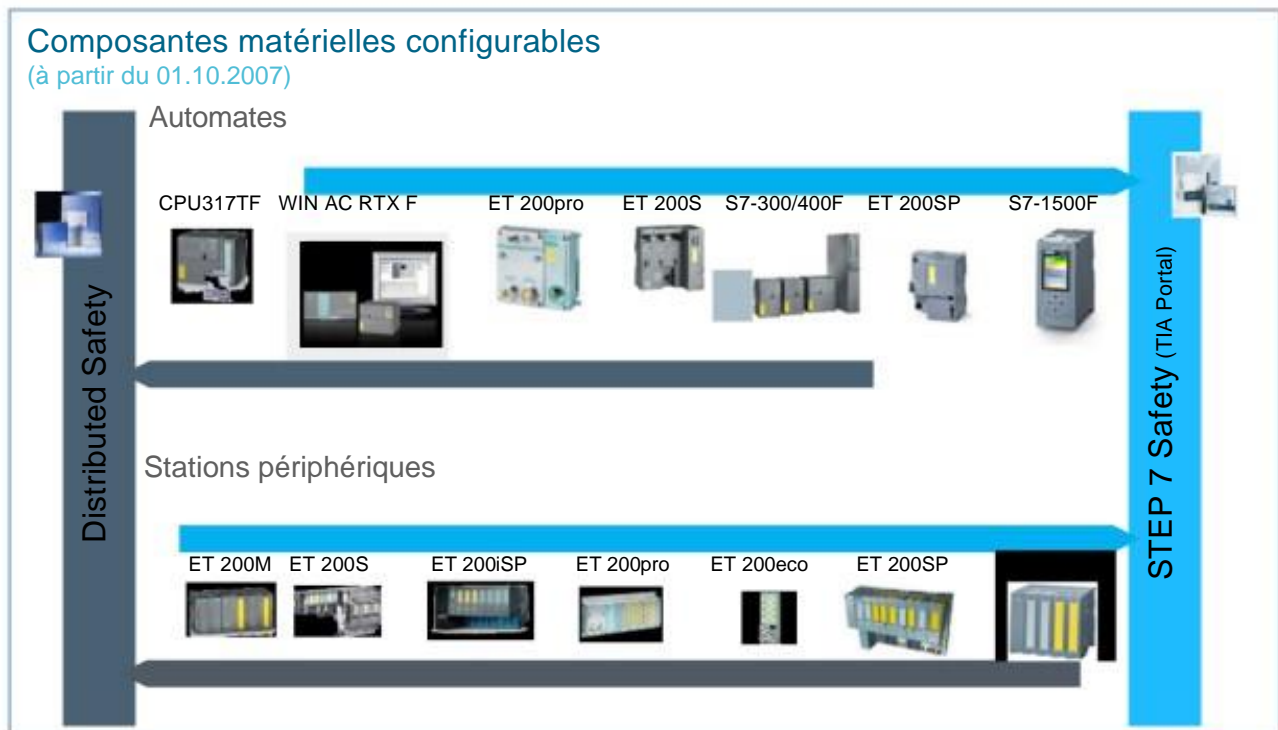


SIMATIC S7

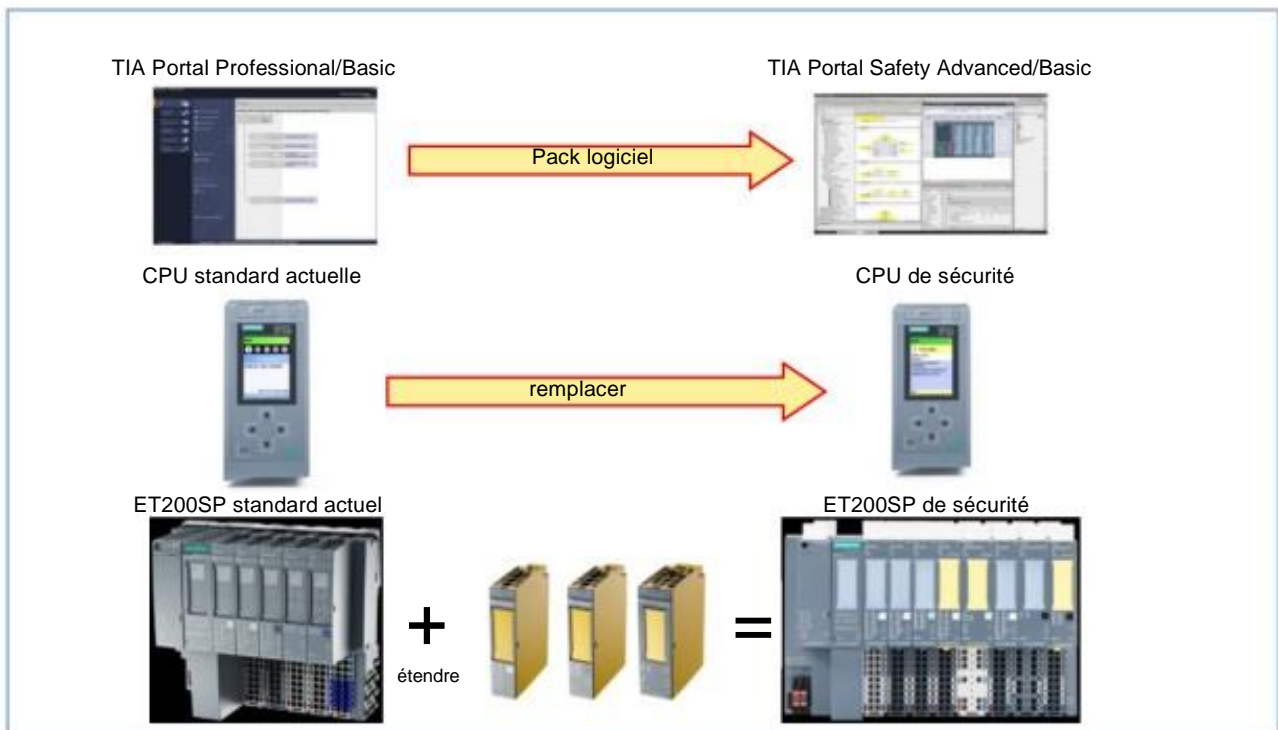
Les contrôleurs S7 se caractérisent par deux niveaux de performance, le niveau de base (S7-1200) et le niveau de performance étendue (S7-1500).

L'ancienne gamme des automates SIMATIC (S7-300 et S7-400) est remplacée par les contrôleurs S7-1200 et S7-1500.

2.2. Composantes matérielles configurables



2.3. SIMATIC Safety Integrated : extensions



CPU F

En général, la CPU F doit répondre aux mêmes exigences que la CPU standard utilisée précédemment en termes de performance et de limites de configuration (y compris les options de communication). Les paramètres les plus importants sont la vitesse de traitement de la CPU car elle donne le temps de cycle donc le temps de réponse du système d'automatisation et la quantité de mémoire de travail qui doit permettre d'exécuter les blocs du programme standard et du programme de sécurité.

DI/DQ F

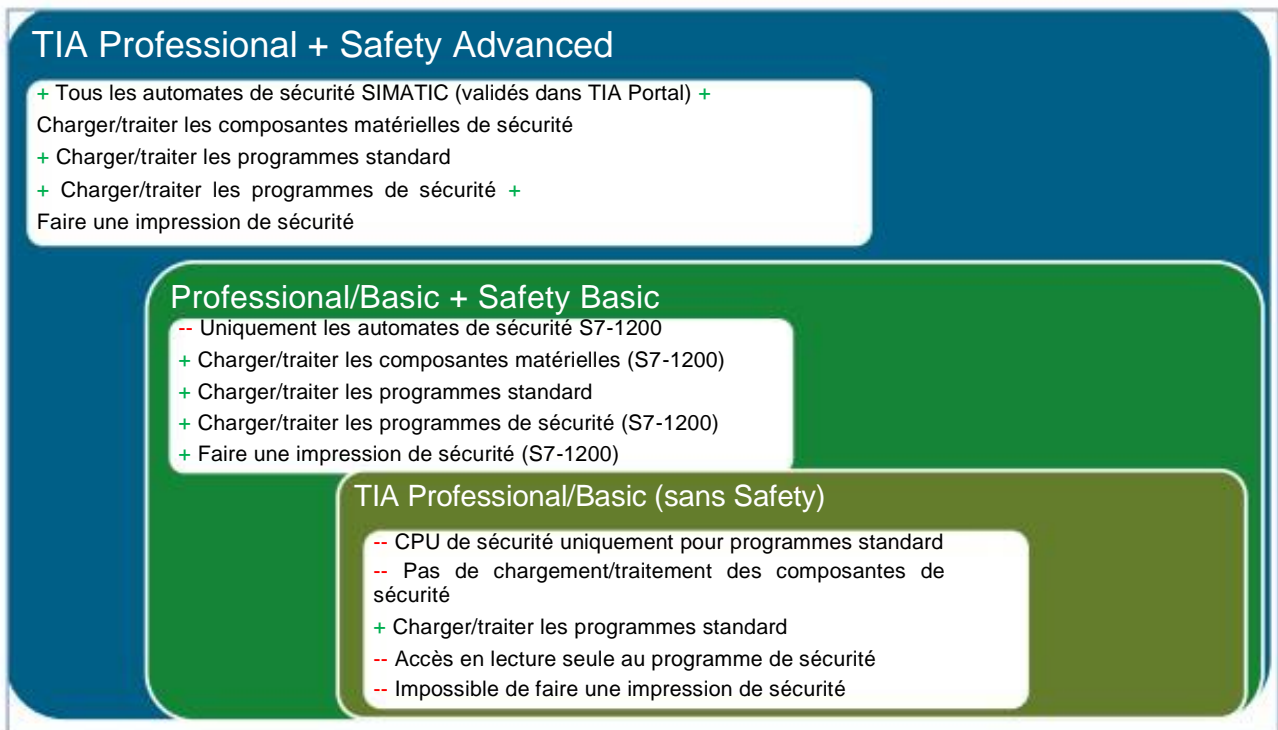
Les modules d'entrée et de sortie standard et de sécurité (F-DI/DQ) peuvent également être utilisés en fonctionnement mixte. Les modules F-DI/DQ nécessaires pour remplacer un relais de sécurité peuvent également être intégrés dans un ET 200SP existant. Tous les modules d'entrée/sortie déjà utilisés, y compris leur câblage, peuvent continuer à être utilisés sans modification.

La première unité de base doit être une unité de base de couleur claire. Une unité de base de couleur claire établit un nouveau groupe de potentiel et une isolation électrique du module adjacent à gauche. La première unité de base de l'ET 200SP est toujours une unité de base de couleur claire pour l'alimentation de la tension d'alimentation L+. Lors de la mise en service, veillez à n'utiliser que des modules de signaux numériques et le module de puissance avec l'unité de base de type A0.






Communication PROFIsafe

La communication de sécurité entre le F-CPU et les modules F-DI/DQ utilisant PROFIsafe est intégrée dans les modules de sécurité. Elle est traitée automatiquement et ne doit pas être programmée, que les modules F-DI/DQ soient utilisés de manière centralisée ou comme modules décentralisés via PROFIBUS ou PROFINET. La communication standard déjà configurée n'est pas affectée par la communication de sécurité via PROFIsafe.

2.4. SIMATIC Safety Integrated : configuration logicielle?



2.5. SIMATIC S7-1200

	1200-CPU				
Types de CPU	1211C	1212FC	1214FC	1215FC	1217C
Interfaces					
Mémoire programme / Mémoire de données	50KB 4 MB	75/100KB 4 MB	100/125KB 4 MB	125/150KB 4 MB	150KB 4 MB
Temps d'exécution (opération sur bit)	85 ns	85 ns	85 ns	85 ns	85 ns
Largeur	90 mm	90 mm	110 mm	130 mm	150 mm

Caractéristiques

- Contrôleur modulaire compact pour applications simples (puissance de calcul faible à moyenne)
- Gamme échelonnée de CPU
- Vaste gamme de modules
- Capacité d'extension jusqu'à 11 modules
- Mise en réseau possible avec PROFIBUS ou PROFINET
- Règles de montage des modules
 - Modules de communication (CM) à gauche de la CPU (en fonction de la CPU) –
 - Modules de signaux (SM) à droite de la CPU (en fonction de la CPU)
- Automatisation complet avec CPU et E/S dans un seul appareil
 - E/S tout-ou-rien et analogiques intégrées
 - Extension avec carte de signaux
- Contrôleur avec fonctions intégrées

2.5.1. SIMATIC S7-1200

Propriétés CPU

Programme de sécurité et applications standard ▪
interface PROFINET

- Fonctions technologiques intégrées : commande de mouvements (Motion), régulation, comptage, mesure
- **Pas d'I/O F sur la base CPU!**
- Profisafe (à partir de V4.1)

Modules E/S S7-1200 à sécurité intégrée

- SM 1226 F-DI 16 x 24VDC
- SM 1226 F-DQ 4 x 24VDC
- SM 1226 F-DQ 2 x Relais



Règles de montage des modules

- Modules de communication (CM) à gauche de la CPU (selon la CPU)
- Modules de signaux (SM) tout-ou-rien et analogiques à droite de la CPU (selon la CPU)

Modules de signaux

- ETOR, STOR, E/S TOR (24V=, relais)
- EANA, SANA ou E/S ANA (tension, courant, résistance, thermocouple)










Modules de communication (CM - Communication module, CP - Communication processor)

- Couplage point-à-point (RS232, RS485)
- PROFIBUS
- Maître AS-i
- Contrôle à distance (fonctionnalité GPRS)

Carte d'extension

- Extension de la CPU avec une périphérie embarquée ou une interface réseau
- Une carte batterie assure la sauvegarde à long terme de l'horloge.

2.6. SIMATIC S7-1500

	ET 200SP		1500 CPUs						T-CPU	MFP CPU
CPU Types	1510SP F-1 PN	1512SP F-1 PN	1511 F-1 PN	1513 F-1 PN	1515 F-2 PN	1516 F-3 PN/DP	1517 F-3 PN/DP	1518 F-4 PN/DP	1511 T 1515 T 1516 T 1517 T	1518 F-4 PN/DP
Interfaces	 1	 1	 1	 1	 1	 1	 1	 1	Comme Standard	 1
Mémoire programme / Mémoire de données	100/150 KB / 750 KB	200/300 KB / 1 MB	150/225 KB / 1 MB	300/450 KB / 1.5 MB	500/750 KB / 3 MB	1/1.5 MB / 5 MB	2/3 MB / 8 MB	4/6 MB / 20 MB	50% de mémoire programme suppl.	4/6 MB / 20 MB / 50 MB ¹⁾
Temps d'exécution (opération sur bit)	72 ns	48 ns	60 ns	40 ns	30 ns	10 ns	2 ns	1 ns	Comme Standard	1 ns
	100 mm	100 mm	35 mm	35 mm	70 mm	70 mm	175 mm	175 mm	Comme Standard	175 mm

1) 50 Mo de mémoire supplémentaire pour les applications ODK (Open Development Kit)

CPU 1510SP F-1 PN à CPU 1518 F-4 PN/DP

Les CPU 1510SP F-1 PN à CPU 1518 F-4 PN/DP sont les CPU de sécurité qui exécutent des applications standards et de sécurité avec des modules de périphéries centralisées ou décentralisées. Elles peuvent être utilisées en tant que contrôleur PROFINET IO ou en tant que module intelligent distribué (PROFINET I-Device). L'interface intégrée PROFINET IO IRT assure la commutation de manière à permettre la réalisation de réseau à topologie linéaire. En outre, les CPU offrent de nombreuses fonctionnalités de régulation et permettent d'intégrer à la solution d'automatisation des systèmes d'entraînement via les blocs standardisés PLC open. Les automates de sécurité S7-151xF sont certifiés selon la norme EN 61508 relative à la sécurité fonctionnelle des systèmes électriques et électroniques programmables (version 2010) et peuvent être utilisées pour des applications de sécurité jusqu'au niveau d'intégrité de sécurité SIL 3, selon la norme CEI 62061 et jusqu'au niveau de performance PLe, selon la norme ISO 13849.

Pour la sécurité de l'information IT, une protection supplémentaire par mot de passe doit être mise en œuvre pour sécuriser la configuration F et le programme de sécurité.

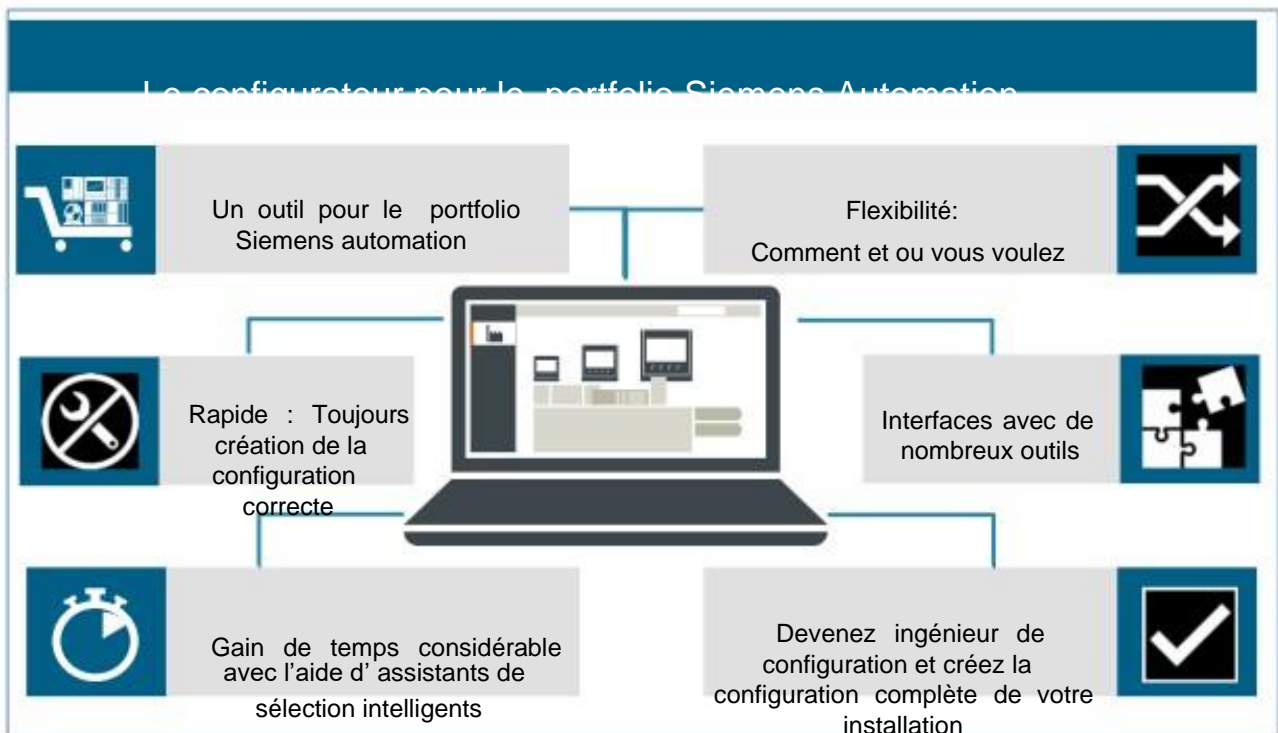
CPU 1518 F-4 PN/DP MFP

Outre la possibilité d'exécuter du code C/C++ dans le programme STEP 7 standard, la plateforme multifonctionnelle CPU 1518(F) MFP fournit un deuxième environnement d'exécution indépendant afin d'exécuter des applications C/C++ en parallèle avec le programme STEP 7 si nécessaire. Le matériel PC supplémentaire précédemment requis n'est plus nécessaire.

2.7. Périphéries de sécurité

Périphérie de sécurité		F-DI	F-DQ PM	F-DQ PP	F-DI/DQ	F-AI	F-PM PM	F-PM PP	F-RO	Propriétés
IP 20	ET 200M	X	X	X	-	X	-	-	-	Périphérie modulaire pour applications nécessitant de nombreuses voies (jusqu'à 24 voies par module)
	ET 200MP	X	X		-	-	-	-	-	Périphérie modulaire pour applications nécessitant de nombreuses voies (jusqu'à 24 voies par module)
	ET 200S	X	X	-	X	-	X	X	X	Périphérie hautement modulaire (jusqu'à 8 voies par module)
	ET 200SP	X	X	X	-	X			X	Périphérie hautement modulaire (jusqu'à 8 voies par module)
	ET 200iSP	X	-	X	-	X	-	-	-	Périphérie hautement modulaire (jusqu'à 8 voies par module) pour une utilisation en atmosphère explosible (zones Ex)
IP 65/67	ET 200pro	X	-	-	X	-	-	X	-	Périphérie modulaire multifonctions en degré de protection élevé
	ET 200eco	X	-	-	X	-	-	-	-	Périphérie décentralisée avec bloc de raccordement en degré de protection élevé

2.8. TIA Selection Tool



TIA Selection Tool

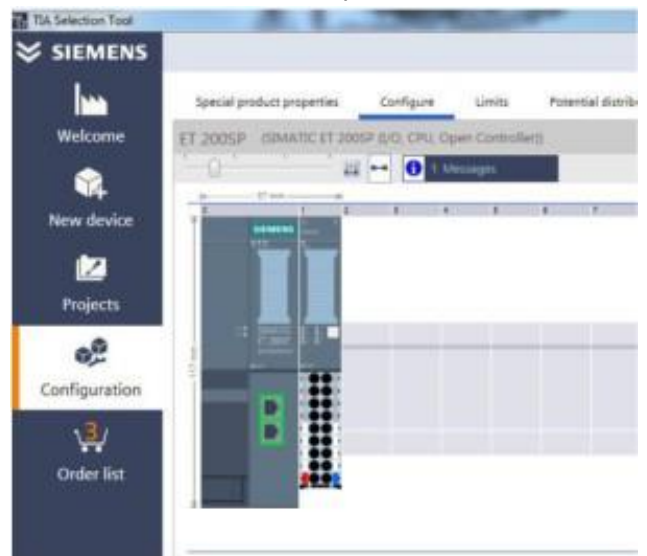
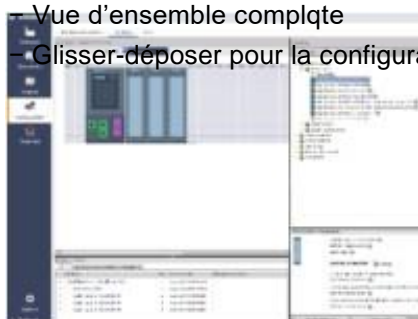
[TIA Selection Tool](#)

Un outil - deux versions

- Hors ligne
 - Tourne localement sur le PC sans Internet
 - Sauvegarde des projets localement ou dans le Cloud
- En ligne
 - Version pour navigateur
 - Optimisé pour le travail mobile et le fonctionnement tactile sur tablette ou portable – Sauvegarde des projets dans le Cloud

Interface utilisateur conviviale

- Pour les appareils tactiles
 - Utilisation rapide et intuitive par le toucher
- Pour les PC
 - Vue d'ensemble complète
 - Glisser-déposer pour la configuration



Interface avec TIA Portal et systèmes ECAD

AutomationML, la nouvelle norme d'échange de données pour les systèmes d'automatisation, permet d'échanger des configurations entre TIA Selection Tool, TIA Portal et les systèmes ECAD (par exemple EPLAN)

- Continuité du travail avec le projet importé immédiatement dans TIA Portal et le système ECAD
- La transition avec l'ingénierie de projet permet de gagner beaucoup de temps

Vue de la charge 24 V DC

Support visuel et technique pour la mise en place d'une alimentation 24 V

- Détermination directe de l'alimentation pour les charges configurées
- Recommandation pour le choix des alimentations adaptées

Interface SIZER

Configuration au-delà des limites de l'automatisation avec l'interface de SIZER

- Passage direct à la configuration de l'entraînement par l'interface de l'outil SIZER
- Les systèmes basse tension, y compris les contrôleurs avec des fonctions motion control, peuvent être configurés et intégrés directement dans les projets dans TIA Selection Tool avec SIZER

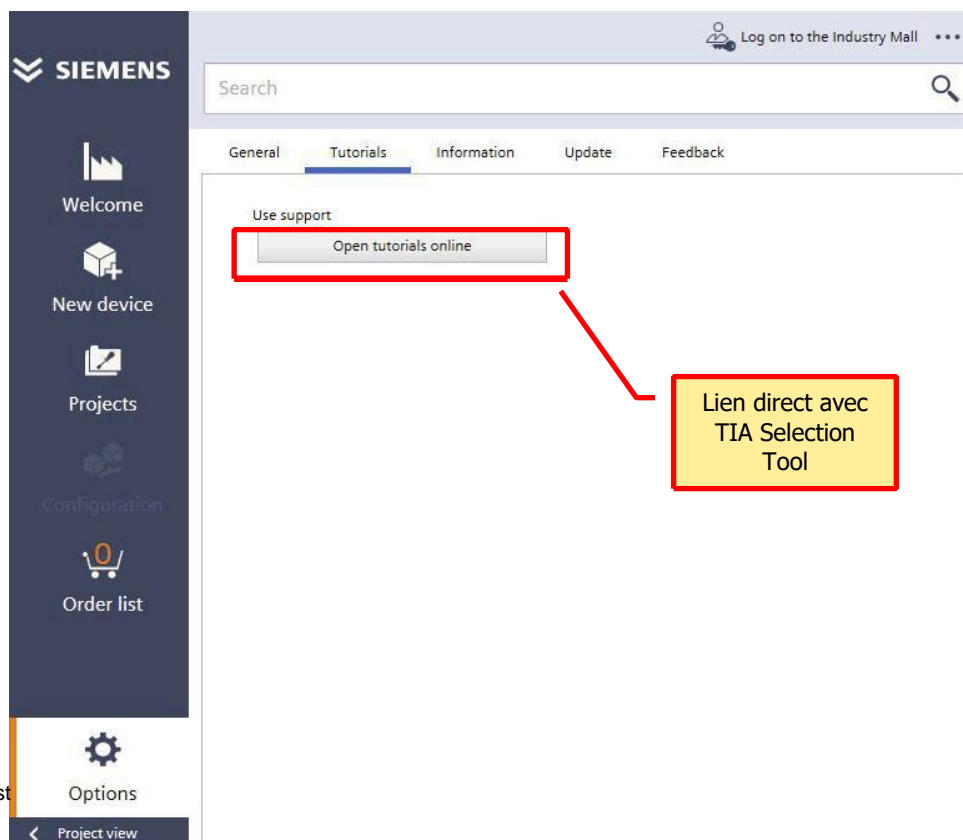
Système modulaire SIRIUS

Permet de combiner de manière optimale

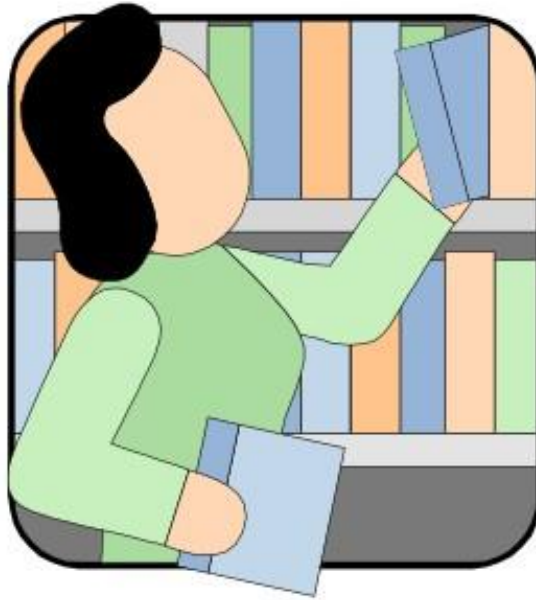
- Mise en place de centaines de départs-moteur
- Vous trouverez tout ce dont vous avez besoin pour commuter, protéger, démarrer et surveiller les moteurs dans le système modulaire SIRIUS

Tutoriels pour toutes les fonctions

Vous disposez d'une quantité de tutoriels pour apprendre à connaître et vous exercer aux fonctions les plus complexes



2.9. Information complémentaire



2.9.1. Contrôleurs ET 200SP et ET 200pro



- Automate SIMATIC S7-1500 sous la forme d'une station périphérique SIMATIC ET 200SP ou ET200pro
- Pour les machines en architecture distribuée et les machines de série installés dans un environnement avec un espace réduit
- Intelligence déportée de l'armoire de commande vers l'automate distribué
- Disponible en version standard et en version de sécurité

2.9.2. Contrôleur logiciel

- Utilisation avec des PC industriels (SIMATIC IPC)
- Fonctionne indépendamment de Windows (même en cas de redémarrage ou de défaillance de Windows)
- Automate flexible pour machines spéciales à hautes performances avec des exigences fonctionnelles élevées
- Intégration des fonctions spécifiques à l'utilisateur via des interfaces ouvertes (par ex. C++ / Matlab)




2.9.3. Contrôleur ET 200SP Open « Tout en un »



- Automate avec E/S modulaires, centralisées
- Visualisation et applications Windows
- Interfaces PC pour écran, souris et clavier
- Gigabit Ethernet

2.9.4. SIMATIC ET 200SP



Pérennité des investissements

- Simple ajout d'un module de sécurité au module de périphérie standard

Mise en service simplifiée

- L'adresse PROFIsafe est configurée par voie logicielle et mémorisée dans le détrompeur.

Remplacement simplifié

- L'adresse PROFIsafe est automatiquement transmise depuis le détrompeur intelligent.

Disponibilité élevée

- Test du signal intégré
- Court-circuit, rupture de fil,...
- Diagnostic simple et rapide grâce aux messages d'erreur clairs et localisation précise des défauts

Utilisation optimale du volume de l'armoire de commande

- Réduction de la largeur du module de 50 % ou plus
- Montage de groupes de potentiel (départs) sans modules de puissance

Modules périphériques de sécurité pour SIMATIC ET 200SP

Le SIMATIC ET 200SP permet d'assurer une communication sécurisée via le réseau PROFIsafe. La taille des modules de sécurité pour entrées/sorties tout-ou-rien (DI et DQ) correspond à celle des modules standard. Leur sécurité fonctionnelle est certifiée conformément à la norme EN 61508. Les modules E/S de sécurité sont conçus pour des applications de sécurité jusqu'au niveau d'intégrité de sécurité SIL 3, selon la norme CEI 62061 relative à la sécurité des machines, et jusqu'au niveau de performance PLe, selon la norme ISO 13849 également relative à la sécurité des machines.

Les modules de sécurité du SIMATIC ET200SP ont une particularité : l'adressage pour les applications de sécurité est réalisé via l'outil d'ingénierie pour l'ensemble de la station périphérique, et non pas via les micro-rupteurs DIP situés sur chacun des modules (adresse F). Ainsi, en cas de remplacement d'un module, l'adresse F (utilisée par les applications de sécurité) enregistrée dans le détrompeur (élément de codage) reste mémorisée dans l'unité de base (Base Unit). En cas d'enchâssage d'un nouveau module sur la CPU, il se voit affecter automatiquement l'adresse F. L'adressage manuel n'est donc plus nécessaire. Le paramétrage est ainsi simplifié, ce qui permet de gagner du temps lors de l'installation d'un nouveau module.

Le module de puissance F-PME du SIMATIC ET 200SP permet d'alimenter des groupes de modules STOR standard ou de sécurité. La fonction de sécurité dans la CPU peut être évaluée au choix dans la CPU de sécurité ou dans le module de puissance F-PM-E. Cette coupure directe et rapide du groupe est assurée jusqu'au niveau d'intégrité de sécurité SIL2 / PLd ou SIL3 / PLe.

2.9.5. Présentation des fonctions de sécurité pour SINAMICS S/G

Entraînement	Fonction de base			Fonctions étendues								
SINAMICS G120/G120C/G120D-2	STO											
SINAMICS G120 F-Version	STO	SS1		SLS	SDI	SSM						
SINAMICS G120D-2 F-Version	STO	SS1		SLS	SDI	SSM						
SINAMICS S110	STO	SS1	SBC	SLS	SDI	SSM	SS2	SOS				
SINAMICS S120 Booksize & Blocksize	STO	SS1	SBC	SLS	SDI	SSM	SS2	SOS	SLP	SP	SBT	
SINAMICS S120 Chassis & Cabinet Modules	STO	SS1	SBC	SLS	SDI	SSM	SS2	SOS	SLP	SP	SBT	
SINAMICS G130/150	STO	SS1	SBC	SLS	SDI	SSM	SS2	SOS	SLP	SP	SBT	
	STO	SS1	SBC	SLS	SDI	SSM	SS2	SOS	SLP	SP	SBT	

Les fonctions de sécurité du système d'entraînement SINAMICS

- STO: Safe Torque Off / Safe Brake Control
- SS1 : Safe Stop 1
- SS2 : Safe Stop 2
- SOS : Safe Operating Stop
- SLS : Safely Limited Speed
- SSM : Safe Speed Monitor
- SDI : Safe Direction
- SBC / SBA : Safe Brake Control / Commande de frein de sécurité
- SP : Safe Position
- SLP : Safe Limited Position
- SBT : Safe Brake Test

Remarques

- Tous les moteurs asynchrones et synchrones 1FU8 (SIMOSYN) peuvent fonctionner sans codeur.
- Si les fonctions de base doivent être commandées via le module TM54F, il faut recourir aux fonctions étendues (Extended Functions) qui comprennent les fonctions de base (Basic Functions).
- Les fonctions de base peuvent également être utilisées sans licence via PROFIsafe.
- Pour les fonctions étendues, il faut acquérir une licence par axe.
- Les fonctions étendues peuvent être commandées par PROFIsafe ou via le module TM54F.

2.9.6. Licences disponibles

Licences disponibles (Industry Mall)

Produit	Article No.
STEP 7 Safety Advanced V15 Télécharger le logiciel	6ES7833-1FA15-0YA5 6ES7833-1FA15-0YH5
Mise à niveau S7 Distributed Safety -> Safety Advanced Télécharger le logiciel	6ES7833-1FA15-0YF5 6ES7833-1FA15-0YY5
SUS STEP 7 Safety Advanced Télécharger le logiciel	6ES7833-1FC00-0YX2 6ES7833-1FC00-0YY0
SUS STEP 7 Safety Advanced compact **	6ES7833-1FC00-0YM2



**SUS compact signifie qu'un seul support de données (une clé USB) est fourni, indépendamment de la quantité commandée.

Tables des matières

3.	Principe de fonctionnement de Safety Integrated.....	3-2
3.1.	Technologies de sécurité conventionnelles	3-3
3.2.	Technologie de sécurité intégrée (Safety Integrated)	3-4
3.3.	Extensions matérielles et logicielles	3-5
3.4.	PROFIsafe	3-6
3.4.1.	Canal noir	3-6
3.4.2.	PROFIsafe	3-7
3.4.3.	Numérotation continue (Compteur).....	3-8
3.4.4.	Surveillance temporelle (Watchdog Timer).....	3-9
3.4.5.	Relation adresse F-Source / adresse F-Destination.....	3-10
3.4.6.	Formation du CRC (Cyclic Redundancy Check)	3-11
3.4.7.	Contrôle du CRC.....	3-12
3.5.	Programme codé.....	3-13
3.5.1.	Traitement codé	3-14
3.6.	Information complémentaire	3-15
3.6.1.	Types d'erreurs	3-16
3.6.2.	Remèdes.....	3-17

3. Principe de fonctionnement de Safety Integrated

→ l'issue de la formation, le participant au stage

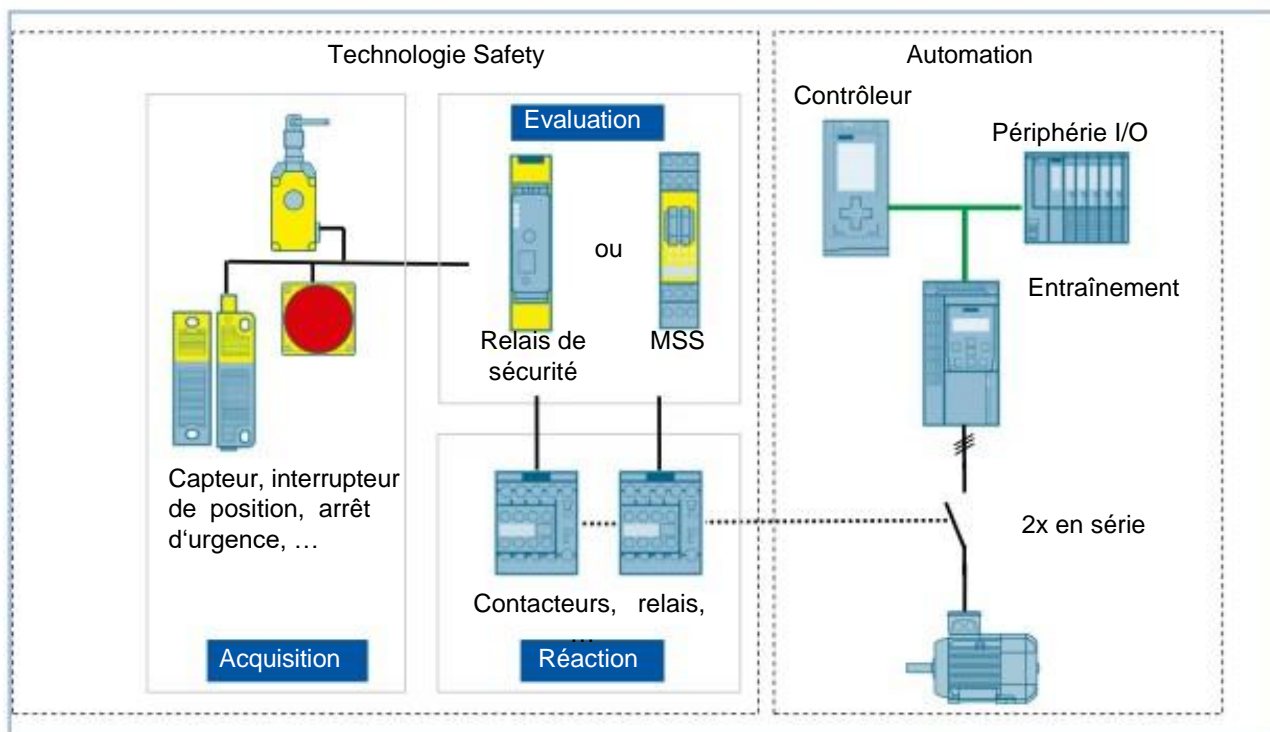
... sera capable d'expliquer le principe de fonctionnement de la sécurité intégrée

... pourra expliquer le principe de la communication PROFIsafe

... pourra expliquer la programmation selon le principe de « redondance diversitaire »



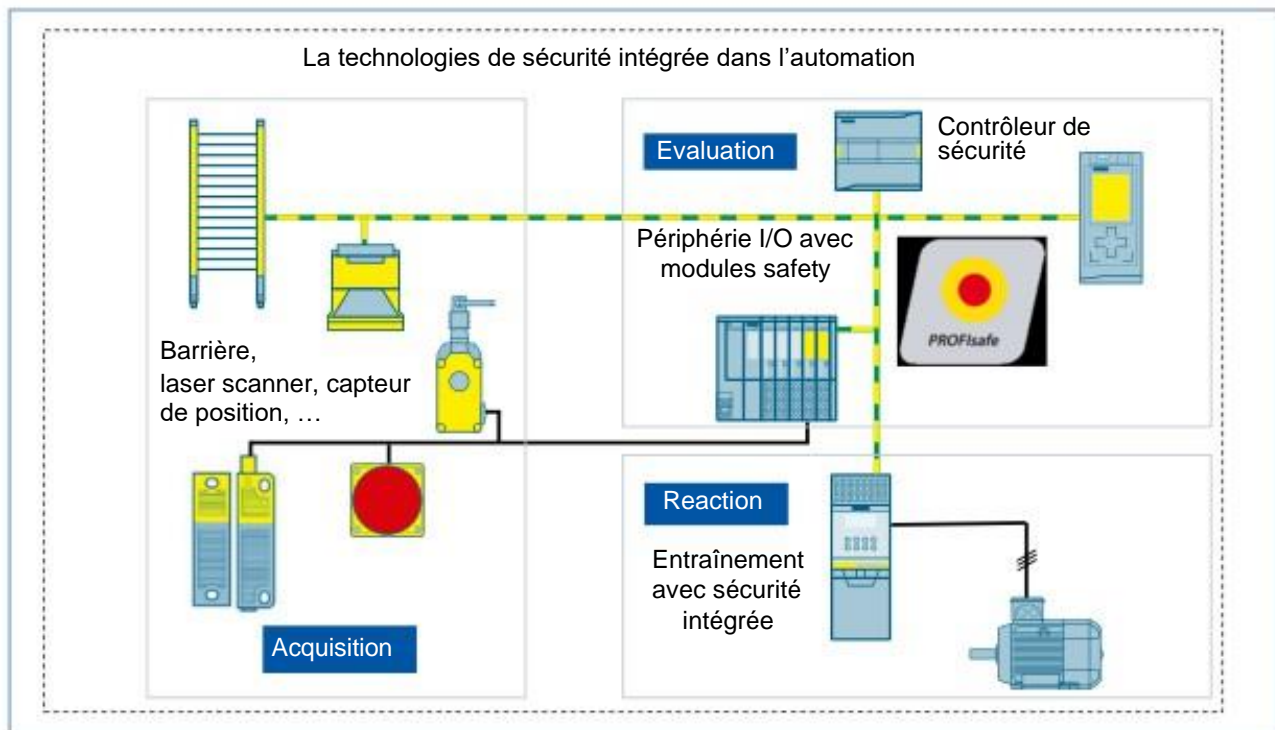
3.1. Technologies de sécurité conventionnelles



Technologies de sécurité conventionnelles

Les fonctions standards et les fonctions de sécurité sont programmées dans des contrôleurs et des réseaux de terrain distincts. Les fonctions de sécurité peuvent être intégrées avec un relais de sécurité ou un contrôleur de sécurité.

3.2. Technologie de sécurité intégrée (Safety Integrated)



Safety Integrated

Safety Integrated désigne le concept de sécurité global destiné aux équipements d'automatisme et aux systèmes d'entraînement de Siemens. Safety Integrated regroupe l'ensemble des composants de sécurité (détecteurs, actionneurs et automates) et intègre la communication sécurisée via un bus de terrain standard. Outre les fonctions standard, les systèmes d'entraînement et les automates peuvent également assurer des fonctions de sécurité. Le concept de sécurité intégrée permet de combiner fiabilité, flexibilité et productivité.

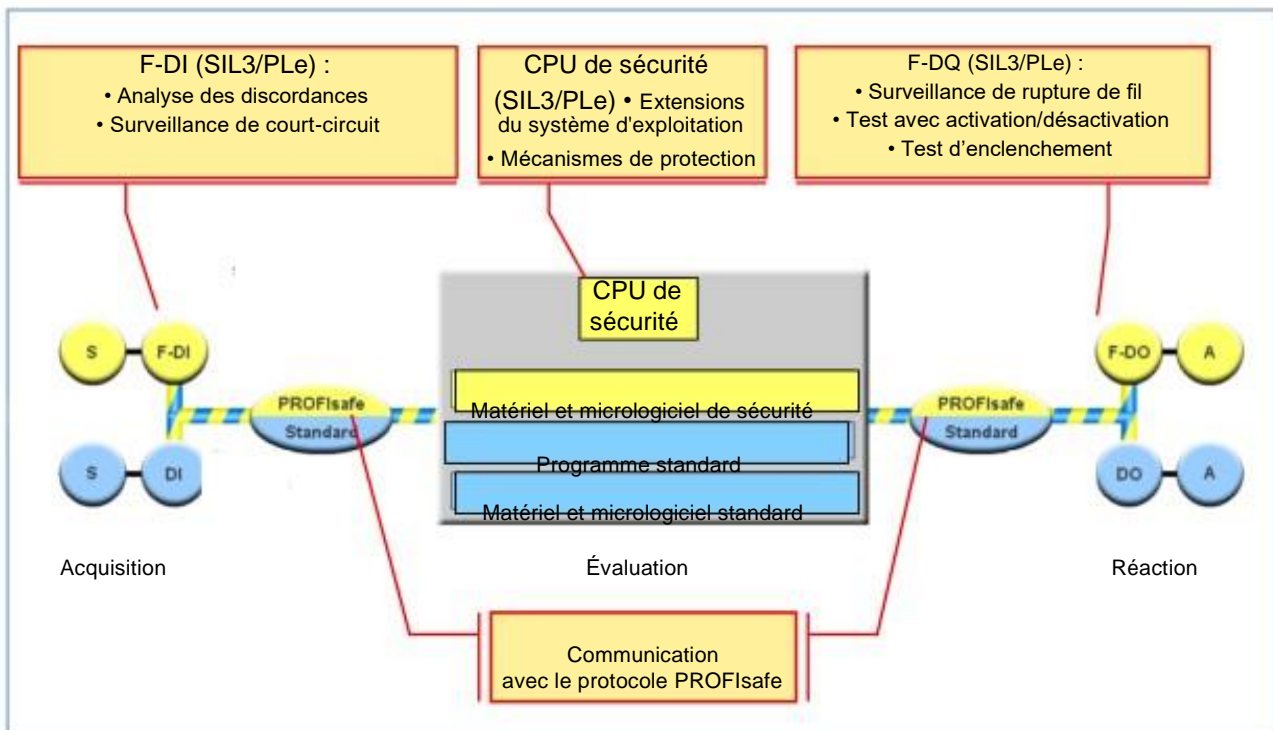
Les équipements d'automatisme standard et les équipements de sécurité sont interconnectés via un système de bus commun. Il peut s'agir d'un réseau PROFIBUS, d'un réseau PROFINET ou d'une combinaison des deux, la communication sécurisée pouvant être également assurée au-delà des limites du bus.

Avantages

Les avantages de l'intégration des applications de sécurité aux systèmes d'automatisation standard sont les suivants :

- Davantage de flexibilité (par rapport aux solutions électromécaniques)
- Réduction des opérations de câblage
- Une seule CPU requise grâce à la coexistence du programme standard et du programme de sécurité
- Communication simple entre le programme standard et le programme de sécurité
- Ingénierie simplifiée (configuration et programmation avec des outils d'ingénierie standard).

3.3. Extensions matérielles et logicielles



Programme standard

Lors de l'intégration des fonctions de sécurité à un automate SIMATIC, les fonctions d'automatisation standard restent pratiquement inchangées :

- Modules de périphérie standard et câblage
- Programme standard

Modules de périphérie de sécurité

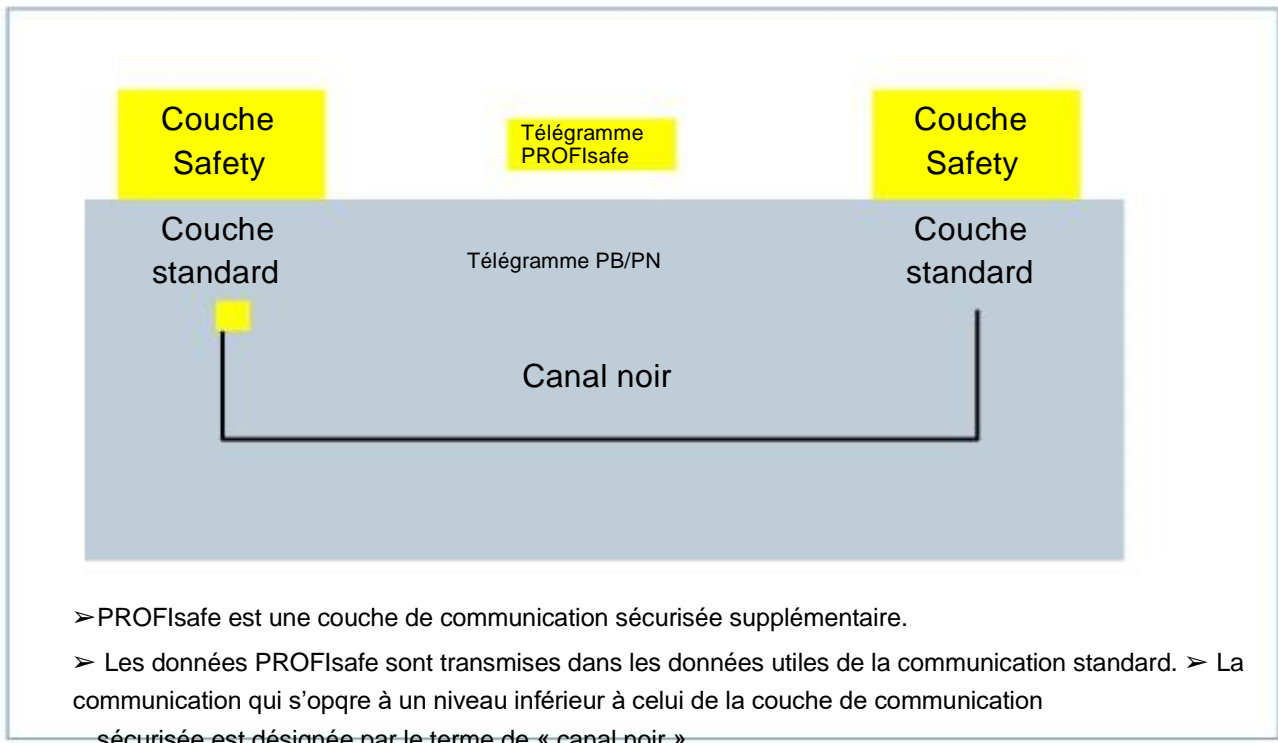
- Les modules de sécurité se distinguent essentiellement des modules standard par leur structure interne à deux canaux. Les deux processeurs intégrés se surveillent mutuellement et testent automatiquement les circuits d'entrée ou de sortie. En cas de défaut, ils font passer le module de sécurité en mode de sécurité.
- Les modules d'entrée tout-ou-rien de sécurité interrogent les états logiques fournis par les détecteurs de sécurité (par ex. : bouton d'arrêt d'urgence), exécutent des tests de court-circuit ainsi que des analyses de discordance, et envoient les télégrammes de sécurité à la CPU F.
- Les modules de sortie TOR de sécurité peuvent commander des manœuvres de coupure avec surveillance de court-circuit jusqu'à l'actionneur.
- Les modules de périphérie de sécurité communiquent avec la CPU de sécurité via le profil de bus de sécurité PROFIsafe.

CPU de sécurité

La CPU standard est remplacée par une CPU de sécurité, qui regroupe les fonctionnalités d'une CPU standard et celles d'une CPU de sécurité. Avec un système d'exploitation doté de mécanismes de protection, des programmes utilisateur standard et des programmes de sécurité peuvent être exécutés sur une même CPU.

3.4. PROFIsafe

3.4.1. Canal noir



Couche PROFIsafe

PROFIsafe est la première norme ouverte pour bus de terrain de sécurité (réseaux de communication industriels CEI 61784) qui permet d'échanger sur un même bus des données standard et des données de sécurité (réseau câblé ou sans fil via un WLAN).

PROFIsafe permet d'assurer la communication standard et la communication de sécurité avec une même infrastructure réseau.

Les données standard et les données de sécurité sont transmises sur la même ligne de bus. PROFIsafe utilise le principe du canal noir pour transmettre les données de sécurité via un réseau standard. Selon ce principe, les données de sécurité transportées sur le réseau de terrain standard sont considérées comme des données supplémentaires (couche PROFIsafe). La communication de sécurité ne dépend donc pas du système de bus et des composantes réseau sous-jacentes.

3.4.2. PROFIsafe

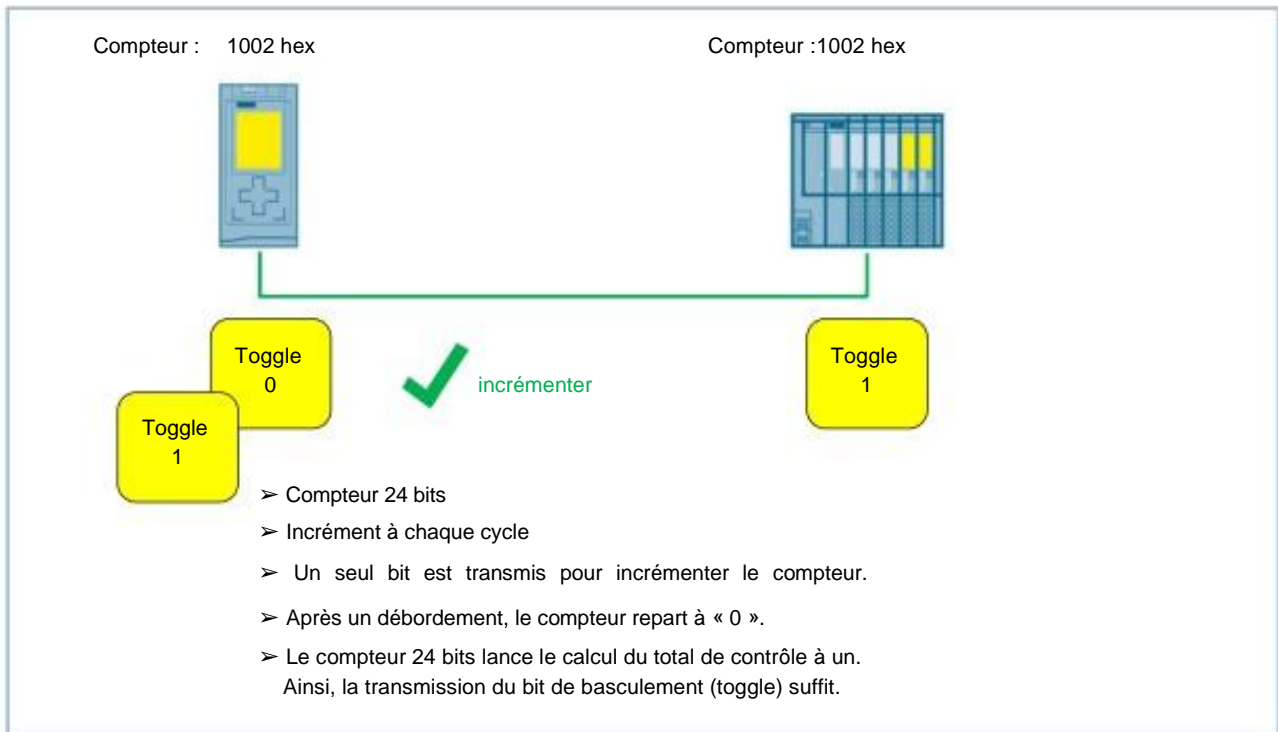
Télégramme PROFIsafe

Données E/S (données utiles)		Octet d'état / de commande	CRC (contrôle de redondance cyclique)
1..12 octet	ou 13..123 octet	1 octet	3 octet ou 4 octets

- Communication de l'automate au périphérique : octet de commande
- Communication du périphérique à l'automate : octet d'état
- Les données d'entrée et de sortie peuvent être étendues à 123 octets.
- 3 ou 4 octets de CRC (en fonction du volume de données à transmettre)

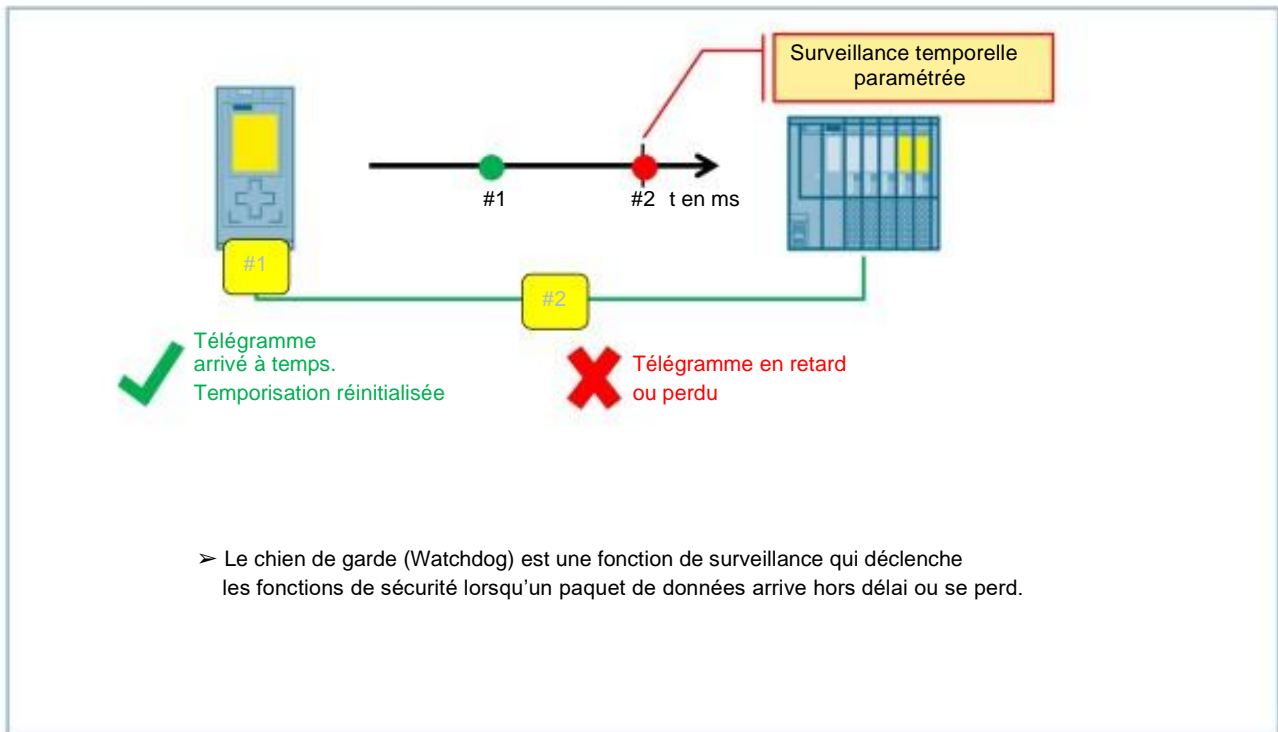
Les données de sécurité échangées entre l'hôte F (CPU de sécurité) et le périphérique de sécurité constituent une charge utile transportée dans les télégrammes PROFIBUS ou PROFINET. Dans le cas d'un périphérique de sécurité modulaire, comportant plusieurs modules de sécurité, la charge utile comprend plusieurs messages de sécurité. Le message commence avec les données d'entrée/sortie. La structure des données d'un périphérique de sécurité est définie dans le fichier GSD correspondant (General Station Description). L'automatisation des processus industriels (que ce soit dans l'industrie manufacturière ou le génie des procédés) soumet le système de commande de sécurité à certaines exigences. La première exigence est le temps de traitement des signaux de sécurité : les signaux (bits) doivent être courts pour pouvoir être traités très rapidement. Les valeurs du processus peuvent avoir un format plus long (virgule flottante) car elles autorisent un temps de traitement plus long. PROFIsafe offre donc deux structures de données différentes : une structure limitée à 12 octets, dont 3 octets pour la signature CRC, et une structure pouvant atteindre 123 octets, avec 4 octets pour la signature CRC. Dans un message de sécurité émis par l'hôte de sécurité, les données d'entrée/sortie de sécurité sont suivies d'un octet de commande (de l'automate) ou d'un octet d'état (du périphérique). Les deux octets permettent de synchroniser les machines utilisant le protocole PROFIsafe. Un télégramme de sécurité se termine par une signature CRC dont la longueur dépend des données d'E/S de sécurité. La numérotation continue n'est pas transmise avec le télégramme de sécurité. L'émetteur et le destinataire disposent de leur propre compteur de télégrammes, qui sont synchronisés à l'aide de l'octet de commande et de l'octet d'état. La synchronisation est surveillée en intégrant la valeur du compteur au calcul de la signature CRC. L'adresse est également surveillée (intégration au calcul de la signature CRC).

3.4.3. Numérotation continue (Compteur)



La numérotation continue des télégrammes permet au destinataire de déterminer si tous les télégrammes sont arrivés et s'ils sont arrivés dans le bon ordre. L'accusé de réception envoyé à l'expéditeur comporte le numéro de télégramme. En fait, un simple bit de basculement (toggle) suffirait pour assurer cette fonction. Mais comme certaines composantes réseau, par ex. les commutateurs, disposent d'une mémoire cache, la communication PROFI-safe utilise un compteur 24 bits.

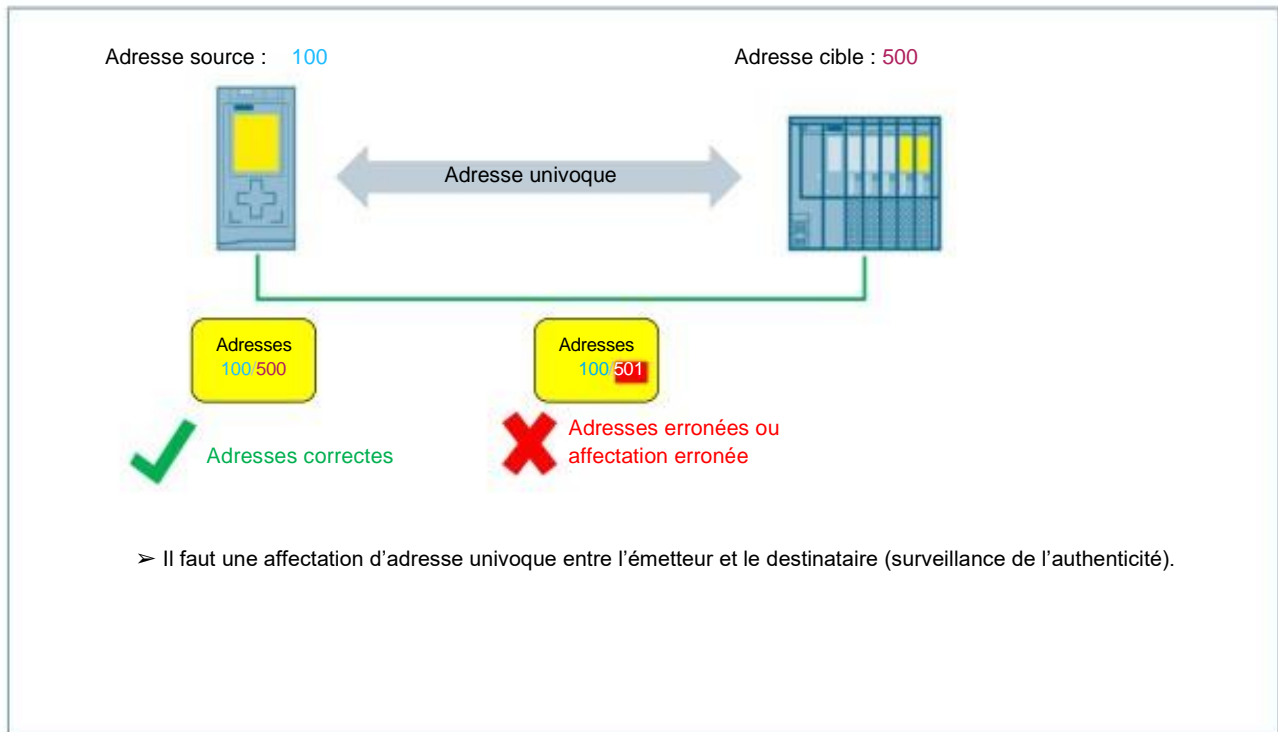
3.4.4. Surveillance temporelle (Watchdog Timer)



Pour les applications de sécurité, il ne suffit pas de transmettre des signaux du processus non corrompus et des valeurs exactes, il convient également de veiller à leur mise à jour dans le délai requis (tolérance aux défauts du processus).

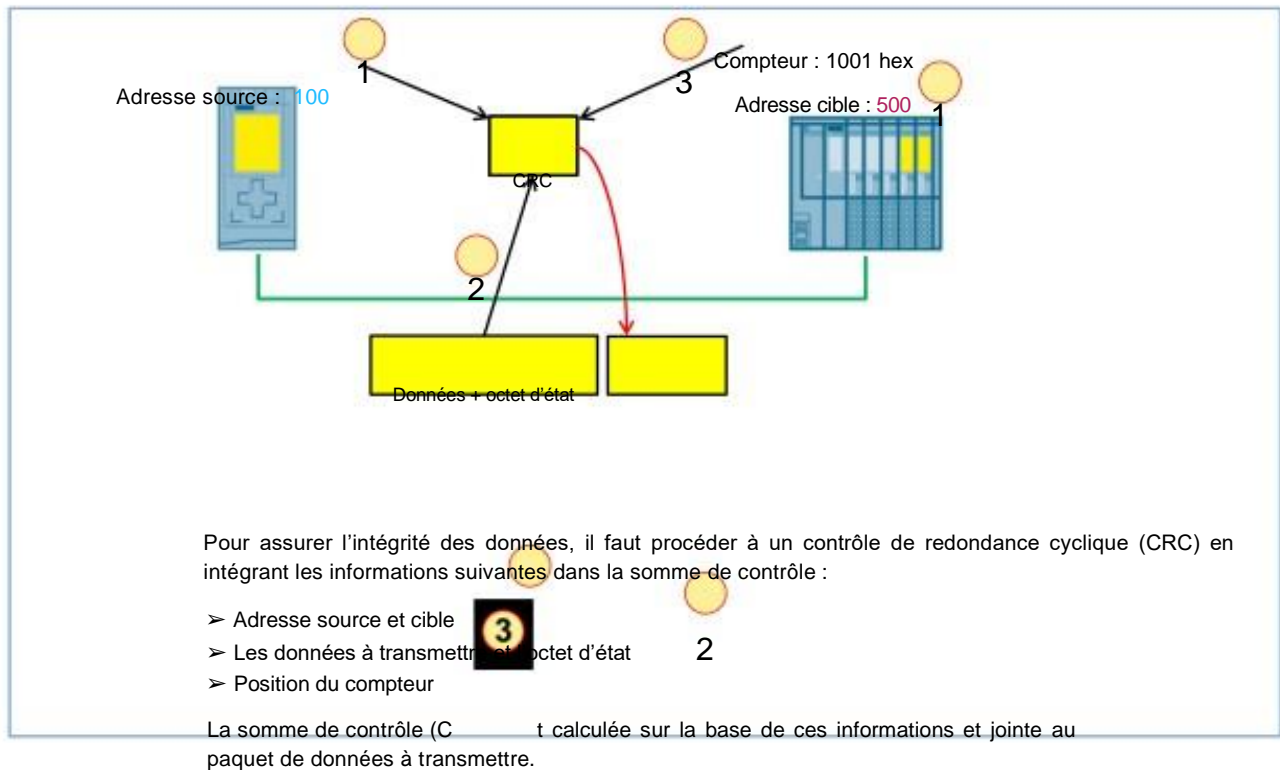
En cas de dépassement du délai imparti, le périphérique de sécurité peut ainsi déclencher par lui-même des mesures de sécurité (arrêt d'un mouvement par exemple). Le périphérique de sécurité utilise une horloge de surveillance (watchdog timer) qui redémarre lorsqu'un message de sécurité arrive avec une nouvelle numérotation continue.

3.4.5. Relation adresse F-Source / adresse F-Destination

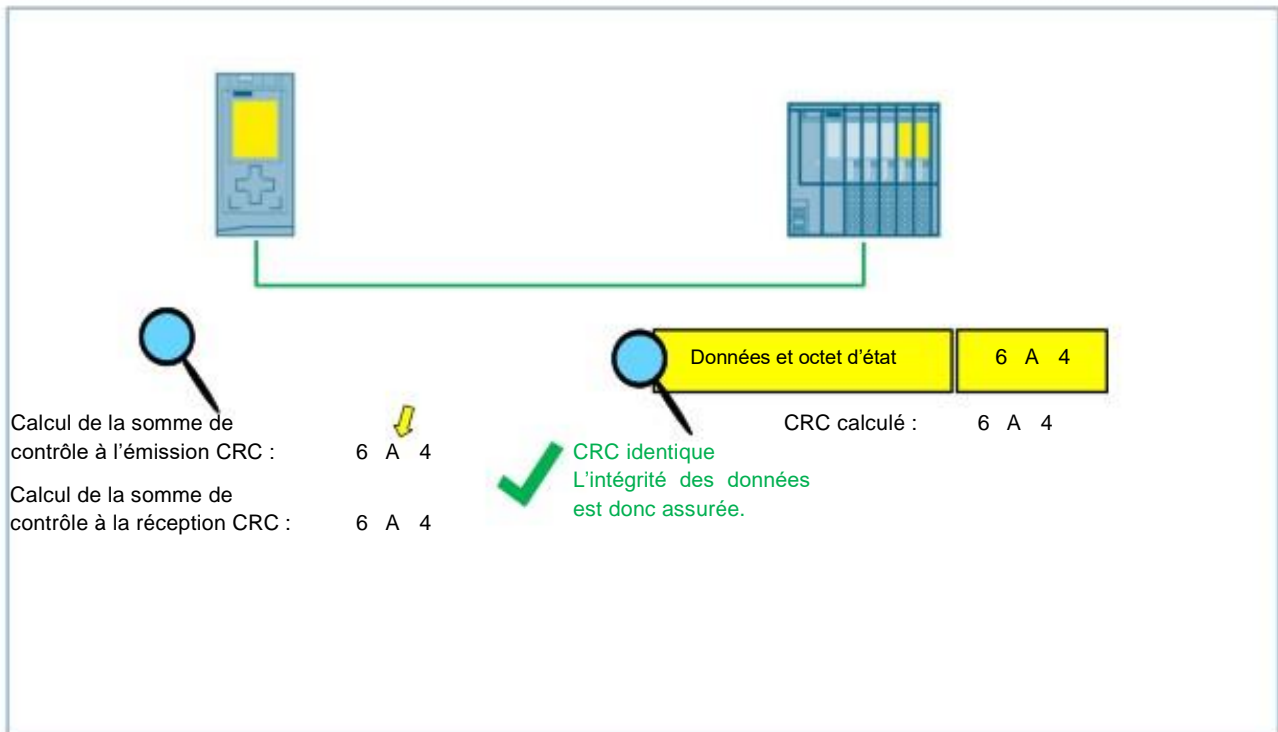


L'authentification de l'émetteur et du récepteur permet à l'automate et à l'appareil de terrain de détecter les messages de sécurité qui ont été acheminés par erreur. Avec PROFIsafe, l'adresse univoque permet d'identifier l'émetteur et le récepteur.

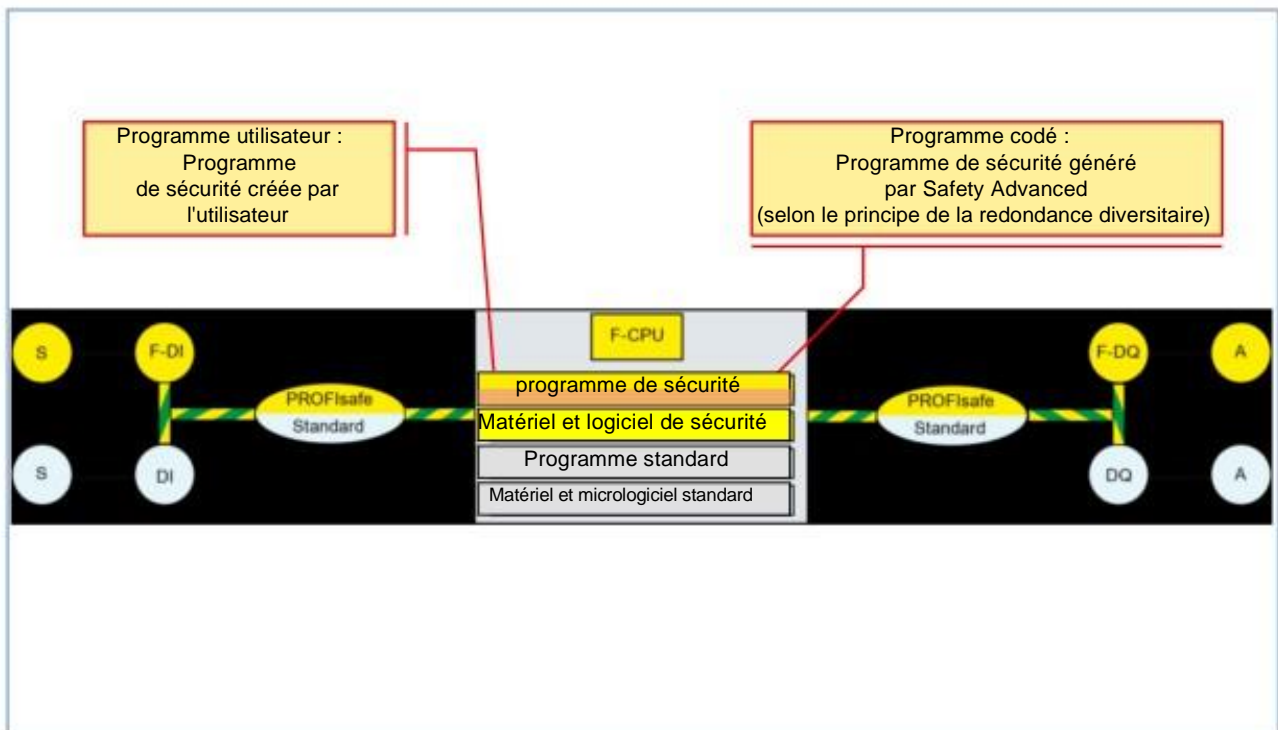
3.4.6. Formation du CRC (Cyclic Redundancy Check)



3.4.7. Contrôle du CRC



3.5. Programme codé



Programme de sécurité

Le programme de sécurité (programme F), qui commande les fonctions de sécurité, se compose d'une séquence de programme créée par l'utilisateur en LOG ou en CONT, et d'une séquence de programme générée par l'outil d'ingénierie Safety Advanced. Cette séquence de programme comporte notamment la logique qui met en œuvre le principe dit de « redondance diversitaire » dans le programme d'automatisation.

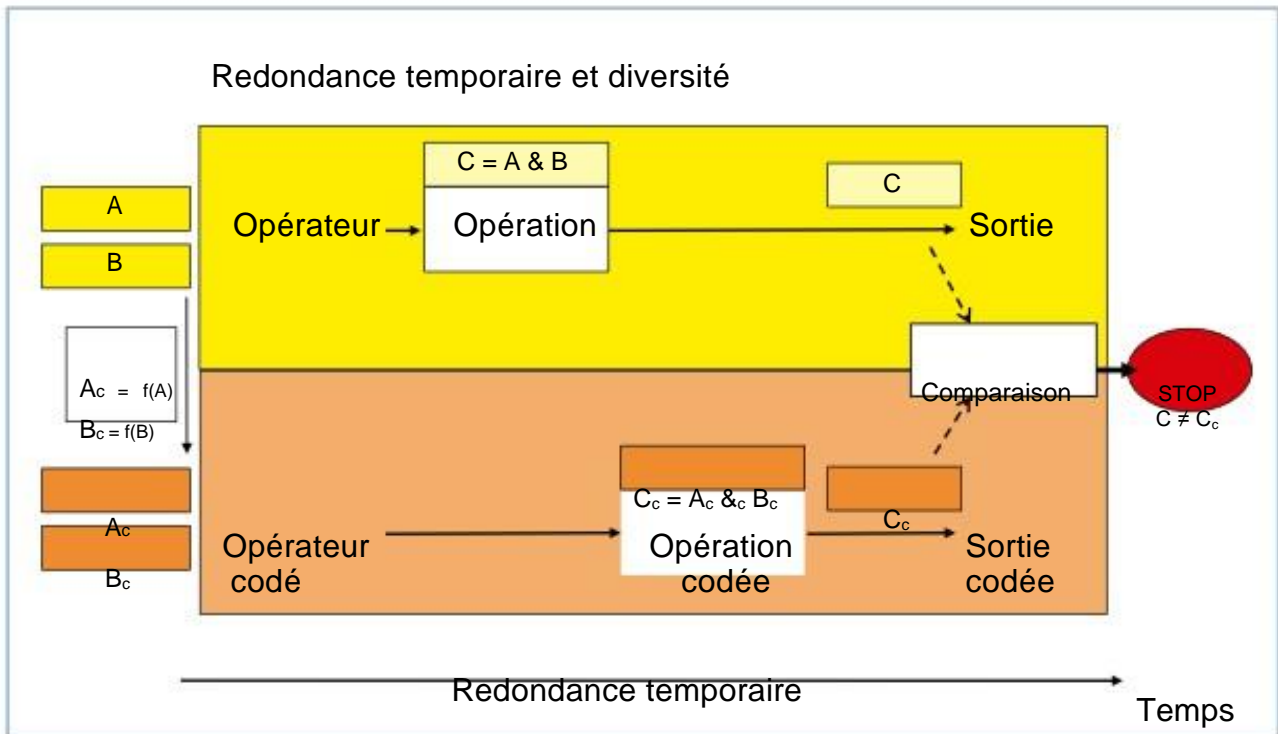
La création du programme standard et du programme de sécurité s'effectue dans le même environnement de programmation. Les blocs fonctionnels certifiés TÜV permettent de réaliser les fonctions de sécurité les plus courantes, ce qui simplifie la programmation.

Coexistence des programmes standard et de sécurité

Les programmes standard et de sécurité sont traités indépendamment les uns des autres par la CPU. En raison de la coexistence des deux programmes sur une même CPU, la communication peut être assurée via des variables globales.

Les modifications du programme standard n'ont aucune incidence sur le programme de sécurité, ce qui permet d'assurer son intégrité.

3.5.1. Traitement codé



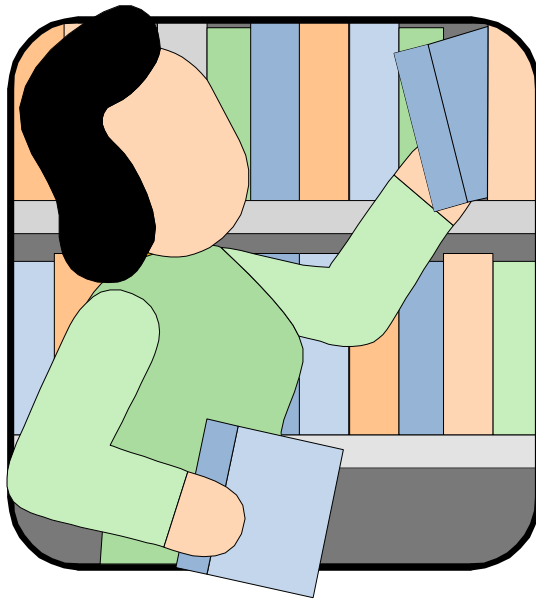
Redondance temporelle et diversité

Les CPU de sécurité du SIMATIC S7 fonctionnent selon les principes de redondance temporelle et de diversité (redondance diversitaire), ce qui permet de mettre en œuvre un système de sécurité avec une seule CPU et un seul processeur. L'outil Safety Advanced ajoute ainsi au programme de sécurité librement programmable par l'utilisateur des blocs de sécurité supplémentaires (FC/FB F). Ils se basent sur une logique « diversitaire » par rapport au programme utilisateur, à savoir une logique qui fait appel à d'autres opérandes et opérations pour obtenir le résultat logique.

Les deux séquences de programme de sécurité sont redondantes dans le temps, ce qui signifie qu'elles sont traitées consécutivement et que les résultats logiques sont comparés. En cas d'erreur, la CPU de sécurité réagit en plaçant l'installation dans un état sécurisé.

En outre, Safety Advanced crée d'autres blocs système de sécurité, qui permettent d'établir la communication PROFIsafe avec les modules de périphérie de sécurité.

3.6. Information complémentaire



3.6.1. Types d'erreurs

Erreur	Description
Répétition	Un paquet obsolète est renvoyé.
Perte	Un paquet est perdu.
Insertion erronée	Un paquet erroné est inséré.
Séquence erronée	Les paquets arrivent dans un ordre erroné.
Corruption des données	Un paquet de données est endommagé ou corrompu.
Retard	Un paquet arrive hors délai admissible.
Mascarade: confusion entre données sécurité et standard	Un paquet de données standard s'apparente à un paquet de données de sécurité.
Adressage (erreur)	Affectation d'adresse équivoque
Erreur de mémoire dans les commutateurs	Erreur de synchronisation FIFO (first in first out)

Récurrence

Des messages obsolètes et non actualisés sont renvoyés au mauvais moment.

Perte

Un message n'est pas reçu ou s'est perdu.

Insertion erronée

Un message d'une source inattendue ou inconnue est inséré.

Séquence erronée

La séquence définie (numéro d'ordre, séquençement) des messages émis par une source donnée est erronée.

Corruption des données

Des messages peuvent être corrompus par un défaut matériel sur une station raccordée au bus, un défaut sur une composante réseau (transmission) ou par un défaut d'intégrité des messages (interférence).

Retard

Des messages peuvent être retardés au-delà de la période de réception admissible, par exemple en raison de défauts de transmission, de la surcharge des liaisons, d'interférences ou de l'envoi de messages qui retardent le service ou qui ne sont pas identifiés (par exemple : FIFO dans les commutateurs, les passerelles et les routeurs).

Confusion des données

Un message provenant d'une source manifestement valide est inséré. Un message standard peut ainsi être reçu par une station assurant une fonction de sécurité. Le message standard est alors considéré comme ayant une incidence sur la sécurité.

Erreur d'adressage

L'affectation d'adresse entre l'émetteur et le récepteur est équivoque.

Erreur de synchronisation dans la mémoire (FIFO) des commutateurs

La séquence de données est erronée

3.6.2. Remèdes

Remède Erreur	Compteur continu(Virtuel)	Surveillance (Watchdog)	CRC (Données)	Adresses source et destination
Répétition	✓			
Perte	✓	✓		
Insertion erronée	✓	✓		✓
Séquence erronée	✓			
Corruption des données			✓	
Retard		✓		
Mascarade		✓	✓	✓
Adressage erroné				✓
Erreur mémoire dans les commutateurs	✓			

Table des matières

4.	Station de travail et configuration matérielle	4-2
4.1.	Structure de la station de travail équipée d'un automate S7-1500F et d'une station périphérique ET200SP	4-3
4.1.1.	Vue synoptique de la station de travail	4-4
4.2.	Configuration matérielle de l'automate de sécurité équipant la station de travail	4-5
4.2.1.	CPU-F dans TIA Portal	4-6
4.2.2.	Sécurité intégrée (Failsafe) et temps de surveillance PROFIsafe (centralisé)	4-7
4.2.3.	Types d'adresse PROFIsafe	4-8
4.2.4.	Temps de surveillance PROFIsafe (décentralisé)	4-14
4.2.5.	Protection de la CPU par mot de passe	4-15
4.3.	Configurer une station périphérique ET 200SP	4-17
4.3.1.	Sélectionner l'unité de base	4-18
4.3.2.	Unité de base pour le module de puissance et le module à relais	4-19
4.3.3.	ET 200SP avec modules de sécurité et modules standard	4-20
4.3.4.	Paramètres de la station périphérique de sécurité	4-21
4.3.5.	Montage et adressage d'un module de périphérie de sécurité ET200SP/MP	4-23
4.3.6.	Attribuer une adresse de sécurité	4-24
4.3.7.	Identifier les modules de sécurité	4-25
4.3.8.	Attribuer une adresse cible	4-26
4.3.9.	État de l'adresse cible	4-27
4.4.	Configurez un IO device avec la détection de matériel	4-28
4.4.1.	Contrôle de configuration (traitement des options) pour la station périphérique de sécurité	4-29
4.5.	Énoncé : Créer un projet et une station matérielle	4-30
4.5.1.	Exercice 1 : Définir l'adresse IP de la PG	4-31
4.5.2.	Exercice 2 : Effacer la carte mémoire SIMATIC (SMC)	4-32
4.5.3.	Exercice 3 : Réinitialiser la CPU et effectuer un redémarrage	4-33
4.5.4.	Exercice 4 : Créer un nouveau projet	4-34
4.5.5.	Exercice 5 : Vérifier les paramètres du projet	4-35
4.5.6.	Exercice 6 : Créer une station S7-1500F	4-36
4.5.7.	Exercice 7 : Propriétés de la CPU - Adresse IP et nom PROFINET	4-37
4.5.8.	Exercice 8 : ET 200SP - Réinitialiser aux paramètres usine	4-38
4.5.9.	Exercice 9 : Détection de l'ET 200SP	4-39
4.5.10.	Exercice 10 : Mettre l'ET 200SP en réseau avec la CPU	4-40
4.5.11.	Exercice 11 : Adaptez la configuration de l'ET 200SP	4-41
4.5.12.	Exercice 12 : Affecter un nom d'appareil et une adresse IP à la station périphérique ET 200SP	4-42
4.5.13.	Exercice 13 : Affecter un nom d'appareil en ligne à l'ET 200SP	4-43
4.5.14.	Exercice 14 : Compiler la configuration matérielle et la charger dans la CPU	4-44
4.5.15.	Exercice 15 : ET 200SP : Attribuer les adresses F	4-45

4. Station de travail et configuration matérielle

→ l'issue de la formation, le participant au stage

... saura configurer les stations de sécurité S7-1500 et ET 200SP.

pourra définir les paramètres généraux d'une CPU et d'un module de sécurité.

... saura affecter les adresses cibles de sécurité.



4.1. Structure de la station de travail équipée d'un automate S7-1500F et d'une station périphérique ET200SP



Station de travail S7-1500F

La station de travail se compose des éléments suivants :

- Automate programmable S7-1500 avec CPU S7-1500F
- Module d'entrée TOR DI 16x24 VDC HF

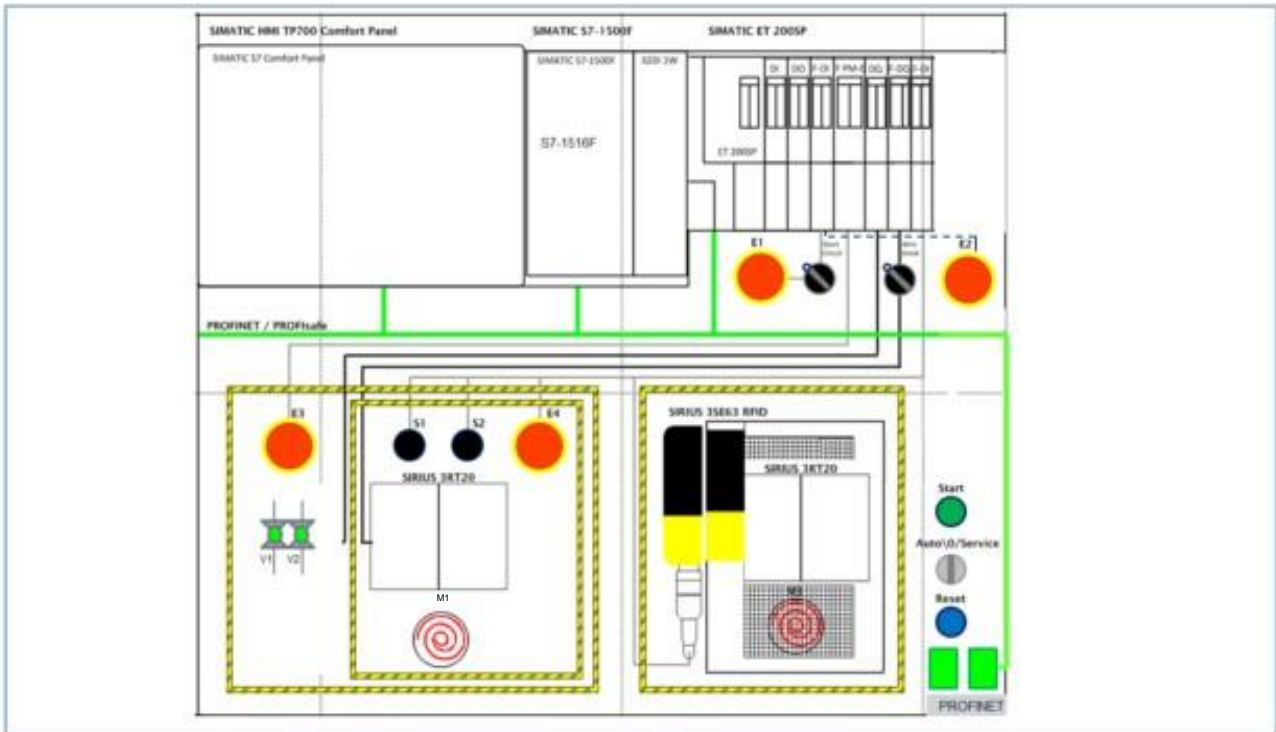
ou

- Automate programmable S7-1500 avec CPU S7-1500F
- Module d'entrée TOR DI 32x24VDC HF
- Module de sortie TOR DQ 32x24VDC/0,5A ST
- Module d'entrée analogique AI 8xUI/RTD/TC ST

ET 200SP

- Station périphérique décentralisée ET 200SP avec interface PROFINET
- Module d'entrée TOR F-DI 8x24VDC, 8 entrées SIL 2/PL d ou 4 entrées SIL 3/PL e
- Module de puissance de sécurité F PM-E PPM DC24V/8A
- Module de sortie TOR F-DQ 4x24VDC/2A PM HF, 4 sorties, commutation PM, SIL 3/PL e
- Module d'entrée TOR F-DI 8x24VDC, 8 entrées SIL 2/PL d ou 4 entrées SIL 3/PL e

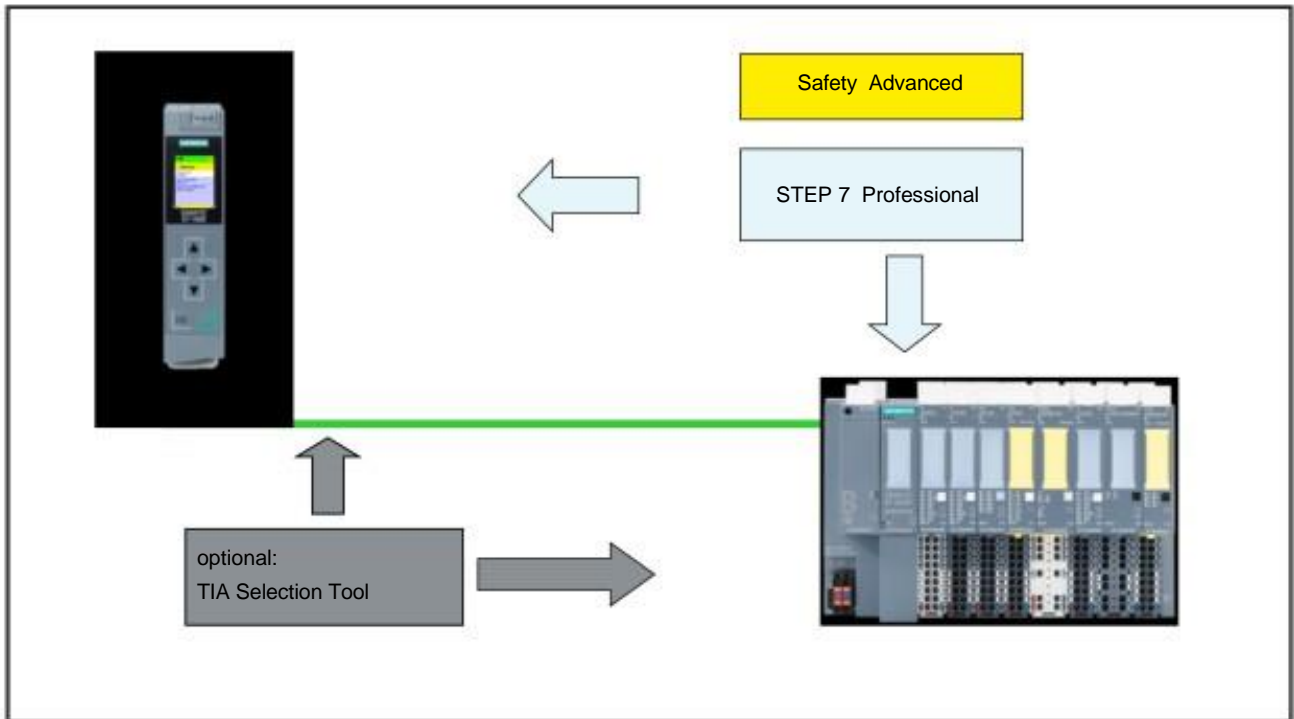
4.1.1. Vue synoptique de la station de travail



Configurer un automate S7-1500F

Un équipement d'automatisme de sécurité SIMATIC Safety se configure généralement de la même manière qu'un système d'automatisation standard S7-1500. Vous configurez et paramétrez le matériel dans l'éditeur « Appareils & Réseaux » en tant que configuration centralisée et/ou décentralisée (ET 200SP). Comme pour un système standard, vous sélectionnez les composants de sécurité dans l'outil « Catalogue du matériel » et vous les placez dans la fenêtre de travail de la « Vue du réseau » ou « Vue des appareils ». Les composants de sécurité sont représentés en jaune.

4.2. Configuration matérielle de l'automate de sécurité équipant la station de travail



Configuration du matériel

La configuration et le paramétrage des modules de sécurité s'effectuent à l'aide de l'outil standard « STEP 7 Professional », la création du programme de sécurité à l'aide du pack « Safety Advanced ».

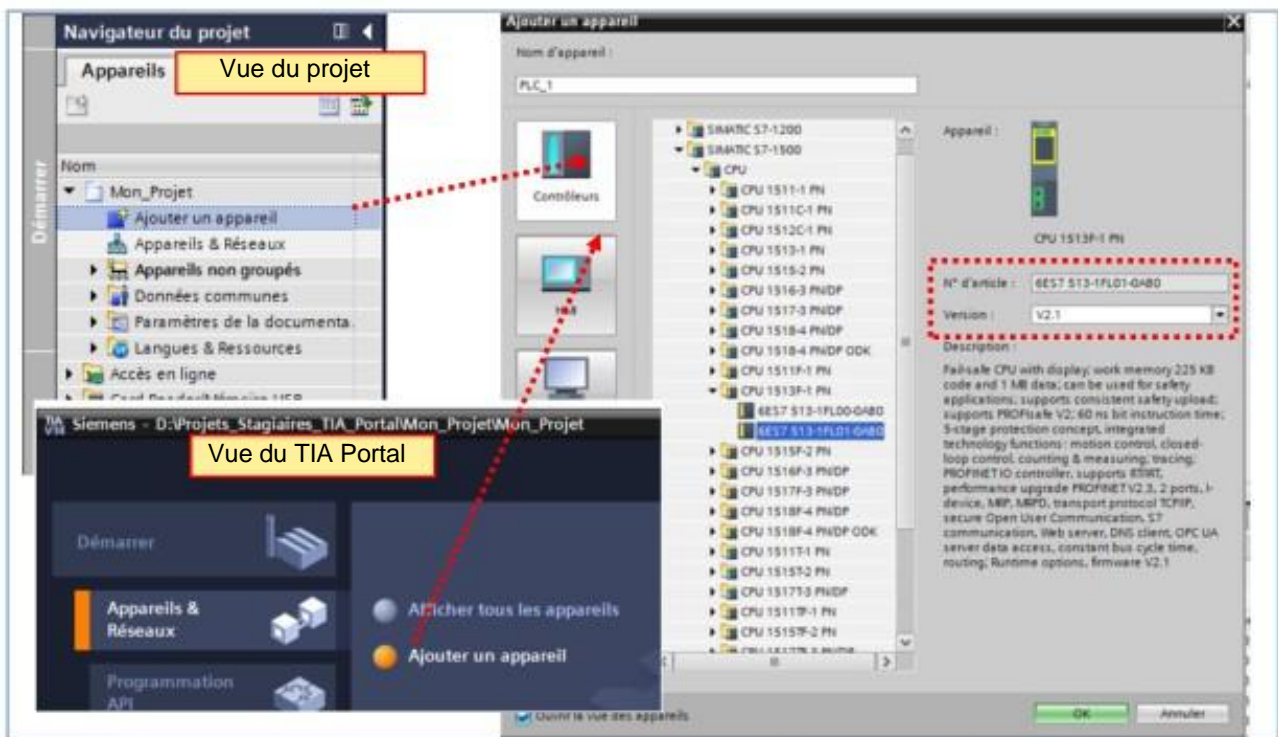
TIA Selection Tool

L'outil TIA Selection Tool permet de sélectionner, de configurer et de commander les équipements d'automatisme de la gamme Totally Integrated Automation. Vous pouvez lancer cet outil directement à partir du Siemens Industry Mall ou le télécharger sous forme de fichier. L'outil TIA Selection Tool propose des assistants pour la sélection des appareils et des réseaux souhaités. Il met également à votre disposition des configurateurs pour la sélection des modules et des accessoires, ainsi que pour la vérification des fonctionnalités.

TIA Selection Tool génère une liste de commande complète à partir de votre sélection ou configuration de produits. Cette liste peut être directement exportée vers le panier de l'Industry Mall ou du catalogue CA 01.

Avec TIA Selection Tool, vous pouvez sélectionner et configurer les composantes de communication industrielle et les logiciels SIMATIC S7, SIMATIC ET 200, SIMATIC IHM, SIMATIC IPC. Vous pouvez également créer des réseaux PROFIBUS et PROFINET, configurer leur topologie et sélectionner les câbles et connecteurs nécessaires.

4.2.1. CPU-F dans TIA Portal



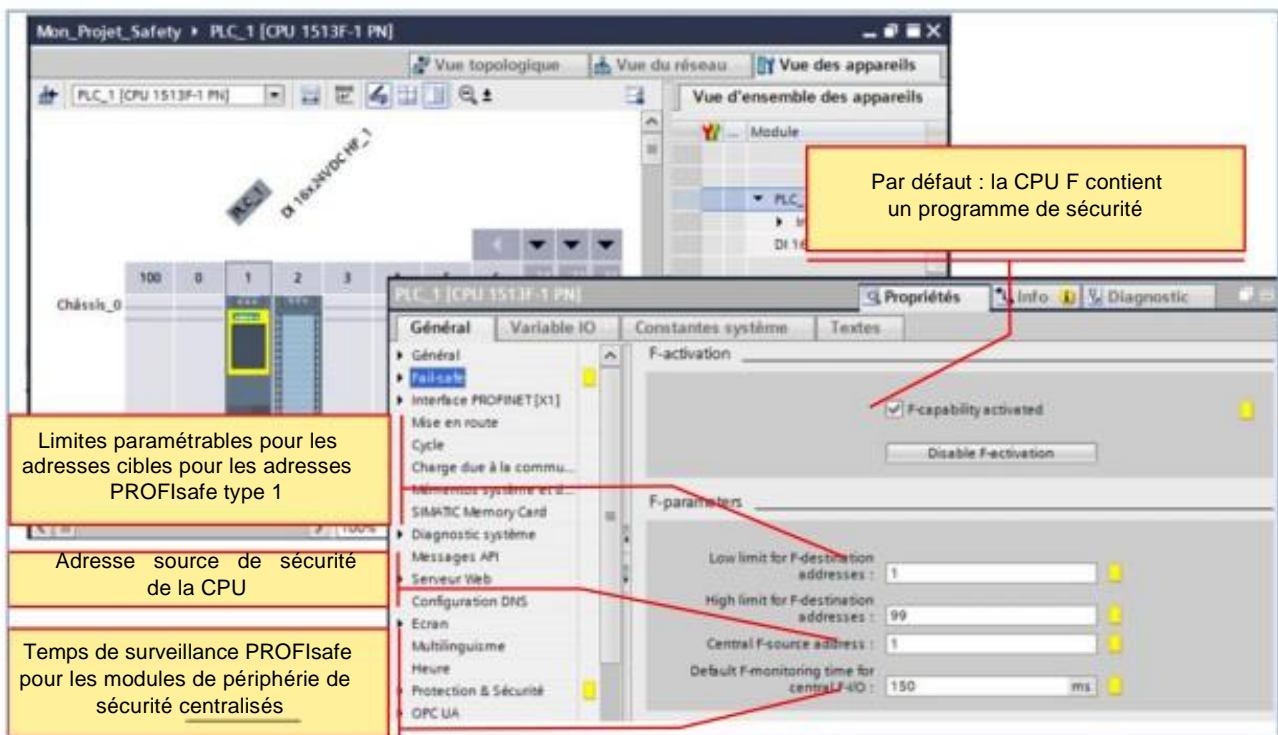
Ajouter un appareil

Vous pouvez créer un nouvel appareil dans le projet avec l'éditeur « Appareils & Réseaux » soit via l'onglet « Catalogue du matériel », soit via l'option « Ajouter un appareil » du Navigateur du projet.

Lors de la création d'un nouvel appareil, un chksis adapté est automatiquement créé. L'appareil sélectionné est enfiché au premier emplacement autorisé du châssis.

Indépendamment du chemin choisi, l'appareil ajouté est visible dans la Vue des appareils et la Vue du réseau de l'éditeur « Appareils & Réseaux ».

4.2.2. Sécurité intégrée (Failsafe) et temps de surveillance PROFIsafe (centralisé)



Activation des fonctions de sécurité

Pour pouvoir charger un programme de sécurité dans la CPU, il faut cocher la case « F-capability activated » (fonctions de sécurité activées). Cette option constitue également une condition préalable indispensable au mode sécurité de la CPU (Failsafe). Elle est activée par défaut. Si elle est désactivée, un programme standard peut continuer à être chargé dans la CPU, mais pas un programme de sécurité.

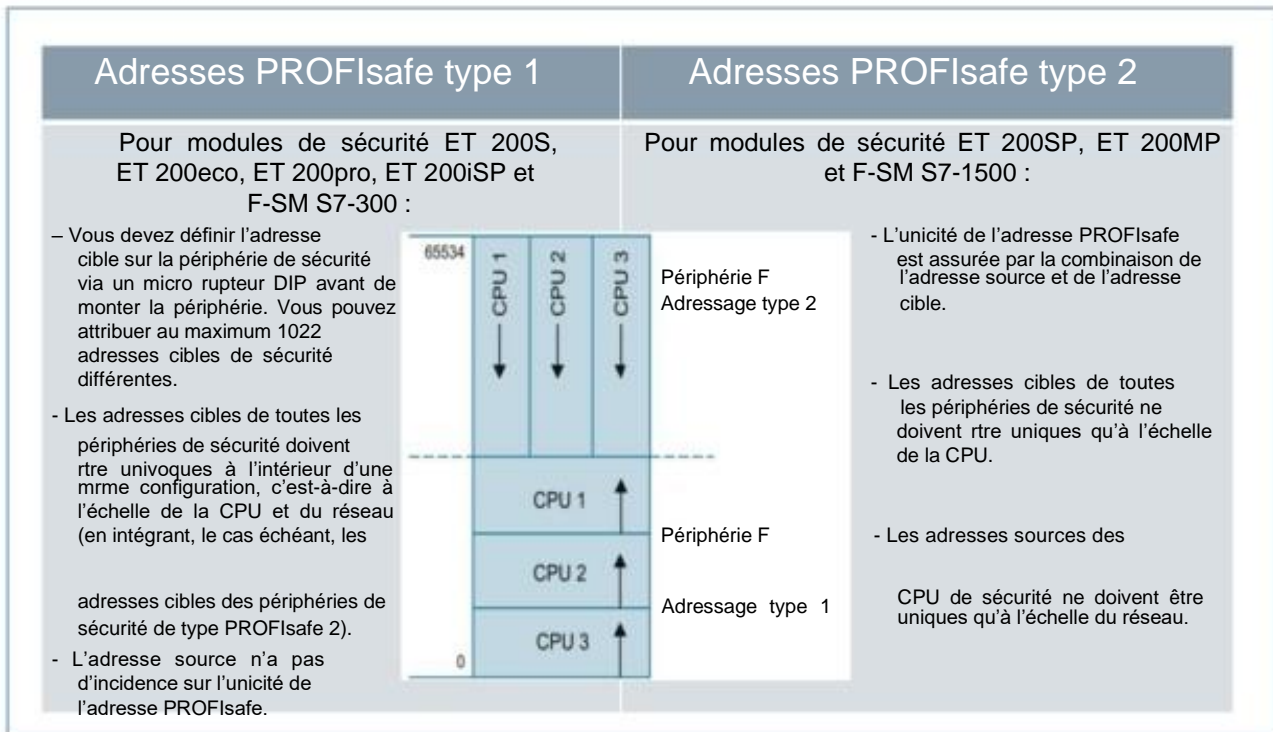
Temps de surveillance par défaut pour la périphérie centralisée

Le temps de surveillance par défaut a une incidence sur la périphérie de sécurité centralisée, qui est montée à côté de la CPU de sécurité (CPU F). Vous pouvez définir ce paramètre dans les propriétés de la CPU F (sélection de la CPU F, puis « Propriétés » > Failsafe > F-parameters »).

Le temps de surveillance de sécurité est le temps de surveillance PROFIsafe pour la communication de sécurité entre la CPU et les modules de signal du châssis central. Si la périphérie ne reçoit aucun télégramme de sécurité valide de la CPU F durant le temps de surveillance paramétré, le module F est passivé et une « erreur de communication » est générée.

Le temps de surveillance PROFIsafe peut au choix être défini manuellement, de manière spécifique pour chaque module, ou de manière centralisée pour tous les modules de périphérie de sécurité, via les paramètres de sécurité de la CPU.

4.2.3. Types d'adresse PROFIsafe



Définir la plage d'adressage cible pour la périphérie de sécurité : adresses PROFIsafe type 1

Avec les paramètres « Limite inférieure des adresses cibles F » (Low limit for F-destination addresses) et « Limite supérieure des adresses cibles F » (High limit for F-destination addresses), vous définissez pour la CPU une plage dans laquelle l'adresse cible sera automatiquement attribuée aux nouveaux modules de sécurité enfichés (adresses PROFIsafe type 1). Une nouvelle adresse cible ne figurant pas encore dans la plage d'adressage cible est également attribuée lorsque vous affectez un nouvel esclave DP/périphérique d'E/S à la CPU F ou lorsque vous activez les fonctions de sécurité de la CPU F.

L'adresse cible est attribuée par ordre croissant à partir de la « Limite inférieure des adresses cibles F ». Si aucune adresse cible libre n'est disponible dans la plage d'adressage cible, la prochaine adresse cible libre en dehors de la plage d'adressage cible est attribuée et un message d'avertissement s'affiche lors de la compilation.

L'adresse cible maximale possible pour les modules de sécurité ET 200S, ET 200eco, ET 200pro, ET 200iSP et F-SM S7-300 est 1022. Les adresses cibles pour la périphérie de sécurité - adresses PROFIsafe type 1 - doivent être univoques à l'échelle du réseau et de la CPU. En choisissant différentes plages d'adressage cible pour différentes CPU F, vous pouvez définir différentes plages pour l'attribution automatique de l'adresse cible. Cela peut être utile lorsque vous exploitez plusieurs CPU F sur un réseau. La modification manuelle des adresses est possible ultérieurement.

Exemple :

Vous avez paramétré la plage d'adressage cible comme suit :

- Limite inférieure des adresses cibles F = 100
- Limite supérieure des adresses cibles F = 199

Lorsque la première périphérie de sécurité - adresse PROFIsafe type1- est montée, l'adresse cible 100 lui est attribuée. Si une périphérie de sécurité supplémentaire - adresse PROFIsafe type 1- est enfichée sur le ckssis, c'est l'adresse cible 101 qui lui est alors attribuée.

Définir la plage d'adressage cible pour la périphérie de sécurité : adresses PROFIsafe type 2

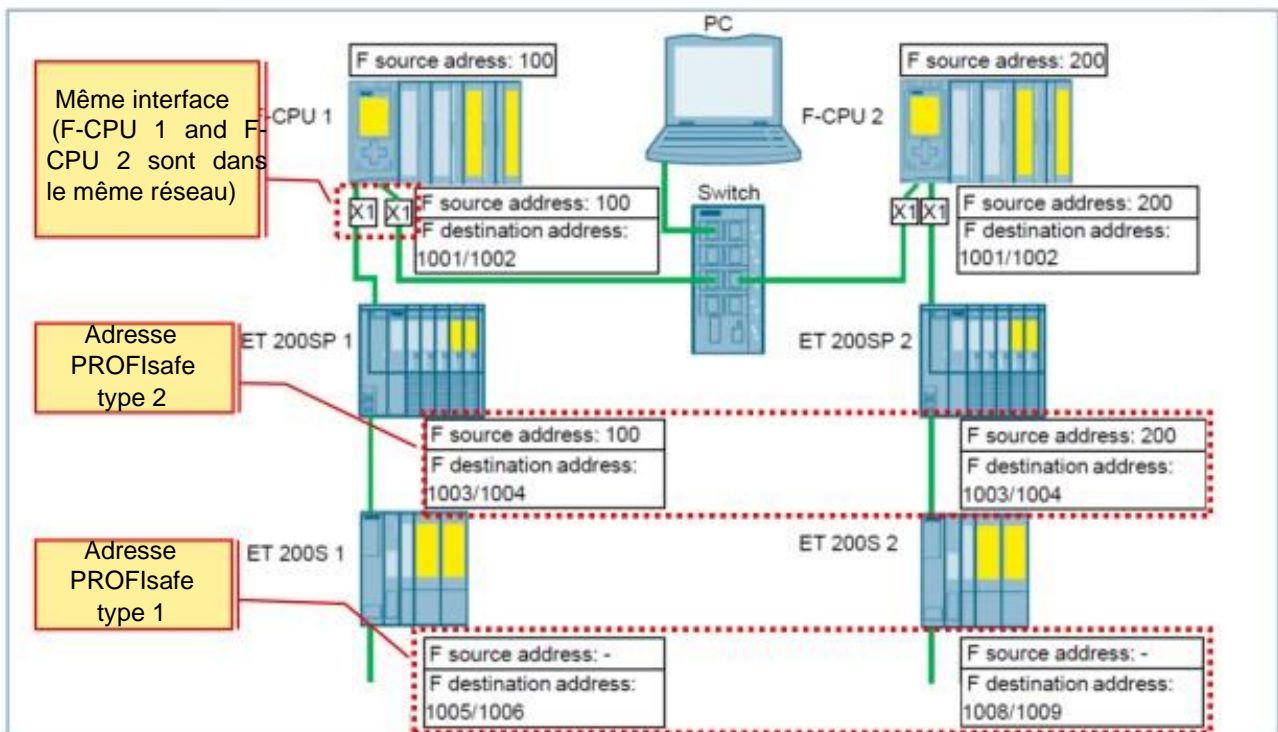
L'adresse cible de la périphérie de sécurité - adresse PROFIsafe type 2 - est automatiquement attribuée pour chaque CPU F par ordre décroissant à partir de 65534. La limite inférieure est la valeur définie dans « Limite supérieure des adresses cibles F » (pour la périphérie de sécurité avec une adresse type 1) + 1.

Lorsque la valeur paramétrée avec le paramètre « Limite supérieure des adresses cibles F » est atteinte, un message d'avertissement s'affiche lors de la compilation.

Définir l'adresse source pour la périphérie de sécurité : adresses PROFIsafe type 2

Le paramètre « Adresse source F centrale » (central F-source address) permet de définir l'adresse source pour la périphérie de sécurité - adresse PROFIsafe type 2 - affectée à la CPU F. L'adresse source doit être univoque à l'échelle du réseau.

4.2.3.1. Configuration d'installation - Exemple 1



La liaison entre les deux sous-ensembles de l'installation s'effectue via l'interface PN X1 sur chaque CPU F. Les deux CPU F sont configurées en tant que contrôleur d'E/S et commandent une périphérie de sécurité connectée via le deuxième port de X1.

Description de la configuration du réseau

La configuration se compose d'un réseau, chaque CPU F pouvant échanger des données avec chacun des participants PROFIsafe via X1. La périphérie de sécurité centralisée ne peut être commandée que via la CPU F correspondante. Elle doit être prise en compte pour l'adressage univoque PROFIsafe à l'échelle de la CPU.

Adresse PROFIsafe type 2

Les périphéries de sécurité des stations ET 200SP appartiennent au type d'adresse 2. Les adresses PROFIsafe obéissent aux règles suivantes :

- Les adresses sources des CPU F doivent être univoques à l'échelle du réseau et
- les adresses cibles F de la périphérie de sécurité doivent être univoques à l'échelle de la CPU.

Comme la CPU F 1 et la CPU F 2 sont sur le même réseau et que leurs adresses sources doivent être univoques à l'échelle du réseau, celles-ci doivent être différentes. Comme l'adresse cible des périphéries ET 200SP ne doit être univoque qu'à l'échelle de la CPU, les adresses cibles de la périphérie peuvent être identiques dans les deux sous-ensembles de l'installation. L'unicité à l'échelle de la CPU concerne les CPU F qui possèdent la même adresse source F que la station périphérique ET 200SP correspondante.

Adresse PROFIsafe type 1

Les périphéries de sécurité des stations ET 200SP et des variateurs SINAMICS appartiennent au type d'adresse 1. L'adresse source ne participe pas à l'unicité de l'adresse PROFIsafe. Les adresses cibles de la périphérie de sécurité doivent donc être univoques à l'échelle de la CPU et du réseau.

Adresses PROFIsafe de la périphérie de sécurité centralisée

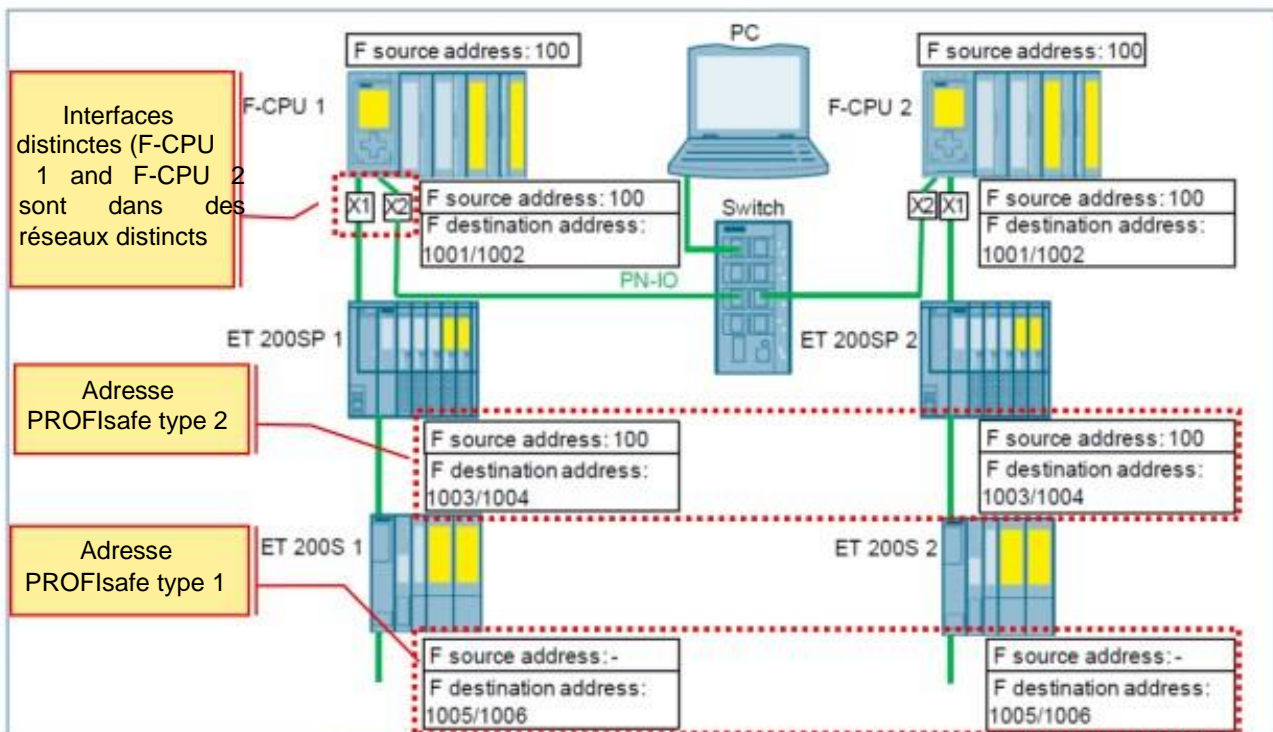
La périphérie de sécurité enfichée sur le châssis central (périphérie centralisée) doit posséder des adresses cibles univoques au sein de la CPU F correspondante. L'unicité à l'échelle de la CPU englobe la périphérie centralisée et la périphérie décentralisée accessible.

Pour la configuration représentée sur la figure ci-dessus, cela signifie :

Les adresses cibles F 1001 et 1002 du châssis contenant la CPU F 1 sont uniques à l'échelle de la CPU et se distinguent des adresses PROFIsafe du réseau formé via X1. Il n'y a pas de chevauchement d'adresses avec la périphérie F centralisée de CPU F 2, car la CPU F 2 ne réalise pas de routage entre X1 et le bus de fond de panier.

Les mêmes principes s'appliquent aux adresses cibles F 1001 et 1002 du châssis contenant la CPU F 2.

4.2.3.2. Configuration d'installation - Exemple 2



Les deux CPU F sont configurées en tant que contrôleur d'E/S et possèdent une périphérie F subordonnée connectée via X1. La liaison entre les deux CPU s'effectue au moyen d'une communication I-Device via l'interface PN X2 (à partir du firmware 2.0).

Description de la configuration du réseau

La configuration se compose, dans la situation initiale décrite au Chapitre 3, de trois réseaux :

- Périphérie de sécurité connectée à l'interface X1 de la CPU F 1
- Périphérie de sécurité connectée à l'interface X1 de la CPU F 2

Liaison PN-IO entre la CPU F 1 et la CPU F 2 via l'interface X2

La périphérie de sécurité centralisée ne peut être commandée que via la CPU F correspondante. Elle doit être prise en compte pour l'adressage univoque PROFIsafe à l'échelle de la CPU.

Adresse PROFIsafe type 2

Les périphéries de sécurité des stations ET 200SP appartiennent au type d'adresse 2. Les adresses PROFIsafe obéissent aux règles suivantes :

- L'adresse source de la CPU F doit être univoque à l'échelle du réseau et
- L'adresse cible de la périphérie de sécurité doit être univoque à l'échelle de la CPU.

La CPU F ne réalisant pas de routage entre les interfaces X1 et X2, les deux CPU F peuvent posséder des adresses sources identiques. Il est néanmoins recommandé d'utiliser des adresses sources différentes. L'utilisation d'adresses différentes est obligatoire lorsqu'une périphérie de sécurité devant être affectée à une CPU F est connectée via l'interface X2.

Comme l'adresse cible des périphéries ET 200SP ne doit être univoque qu'à l'échelle de la CPU, les adresses cibles de la périphérie peuvent être identiques dans les deux sous-ensembles de l'installation.

Adresse PROFIsafe type 1

Les périphéries de sécurité des stations ET 200SP et des variateurs SINAMICS appartiennent au type d'adresse 1. L'adresse source ne participe pas à l'unicité de l'adresse PROFIsafe. Les adresses cibles de la périphérie de sécurité doivent donc être univoques à l'échelle de la CPU et du réseau.

Aucun routage n'étant réalisé entre les interfaces X1 et X2, les adresses cibles peuvent être identiques dans les deux sous-ensembles de l'installation.

Adresses PROFIsafe de la périphérie de sécurité centralisée

La périphérie de sécurité enfichée sur le châssis central (périphérie centralisée) doit posséder des adresses cibles univoques au sein de la CPU F correspondante. L'unicité à l'échelle de la CPU englobe la périphérie centralisée et la périphérie décentralisée accessible.

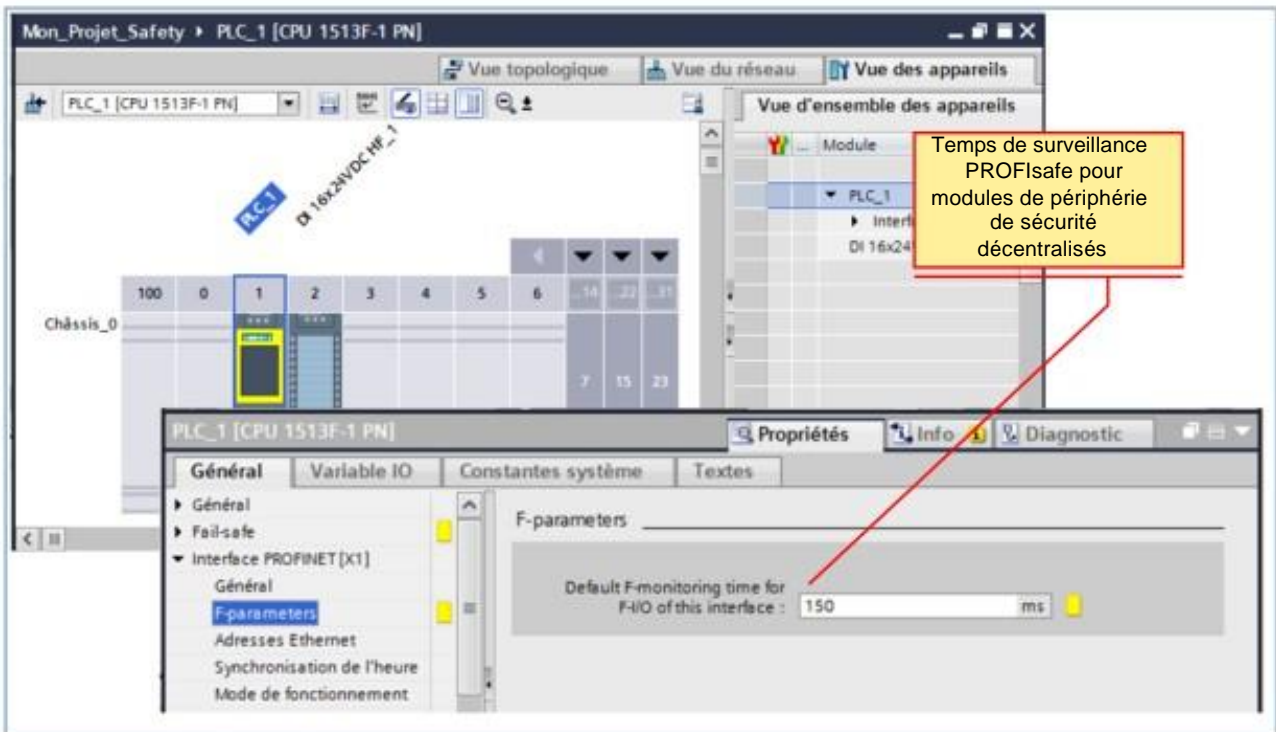
Pour la configuration représentée sur la figure ci-dessus, cela signifie :

Les adresses cibles 1001 et 1002 du châssis contenant la CPU F 1 sont uniques à l'échelle de la CPU et se distinguent des adresses PROFIsafe du réseau formé via l'interface X1. Aucun routage n'étant réalisé au niveau de la CPU F 2 entre les interfaces X1 et X2, la CPU F 1 ne peut pas accéder à la périphérie de sécurité affectée à la CPU F 2.

Il n'y a pas de chevauchement d'adresses de la périphérie de sécurité de la CPU F 1 avec la périphérie de sécurité centralisée de la CPU F 2, car aucun routage n'est réalisé au niveau de la CPU F 2 entre le bus de fond de panier et l'interface locale X2.

Les mêmes principes s'appliquent aux adresses cibles 1001 et 1002 du châssis avec la CPU F 2.

4.2.4. Temps de surveillance PROFIsafe (décentralisé)



Temps de surveillance F par défaut pour la périphérie décentralisée

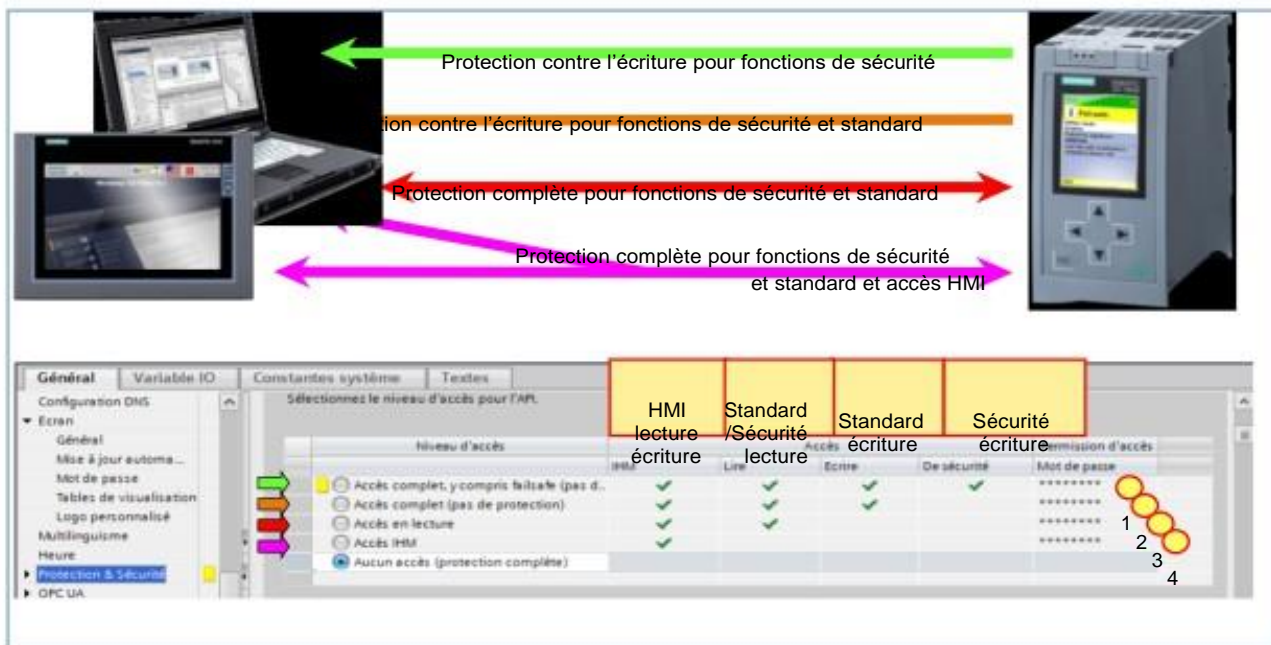
Le temps de surveillance par défaut pour la périphérie de sécurité de cette interface (Default F-monitoring time for F-I/O of this interface) a une incidence sur l'ensemble de la périphérie affectée à cette interface de la CPU F (PROFIBUS ou PROFINET). Vous pouvez modifier ce paramètre dans les propriétés de l'interface correspondante (sélection de l'interface dans l'onglet « Vue d'ensemble des appareils », puis « F-parameters » - paramètres de sécurité).

Grâce aux différentes possibilités de paramétrage, vous pouvez adapter le temps de surveillance aux conditions de votre système de sécurité, par ex. pour tenir compte des différents cycles de bus.

Le temps de surveillance est le temps de surveillance PROFIsafe pour la communication de sécurité entre la CPU F et la périphérie décentralisée. Si la périphérie de sécurité ne reçoit aucun télégramme de sécurité valide de la CPU F durant le temps de surveillance paramétré, le module de sécurité est passivé et une « erreur de communication » est générée.

Le temps de surveillance peut être défini manuellement, de manière spécifique pour chaque module, ou de manière centralisée pour tous les modules de périphérie via les paramètres F de la CPU.

4.2.5. Protection de la CPU par mot de passe



Niveaux de protection

Les niveaux de protection suivants permettent de définir les droits d'accès (en lecture/en écriture) du système de programmation à la CPU :

- **Accès complet, y compris failsafe (pas de protection) :** → réglage par défaut sur les CPU F
L'accès en lecture et en écriture est toujours autorisé.
- **Accès complet (pas de protection) :** → réglage par défaut sur les CPU standard
L'accès en lecture est toujours autorisé, l'accès en écriture n'est possible que vers le programme standard.
- **Accès en lecture :** → protection contre l'écriture, accès possible uniquement en lecture
Sans entrée d'un mot de passe, aucune donnée ne peut être modifiée dans la CPU, de même qu'aucun bloc ni aucune configuration matérielle ou paramétrage modifiés ne peut être chargé dans la CPU.
- **Accès IHM :** → protection contre l'écriture et la lecture pour STEP7
Aucun accès en écriture et en lecture n'est possible à partir du système d'ingénierie. Seuls peuvent être affichés dans le Navigateur du projet, sous « Abonnés accessibles », le type de la CPU et les données d'identification. L'affichage d'informations en ligne ou de blocs sous « Abonnés accessibles » n'est pas possible sans l'entrée d'un mot de passe.
- **Aucun accès (protection complète) :** → protection générale contre l'écriture et la lecture pour STEP7 et appareils IHM. L'accès aux appareils HMI du réseau n'est à présent plus possible sans mot de passe configuré.

Autorisation d'accès par mots de passe

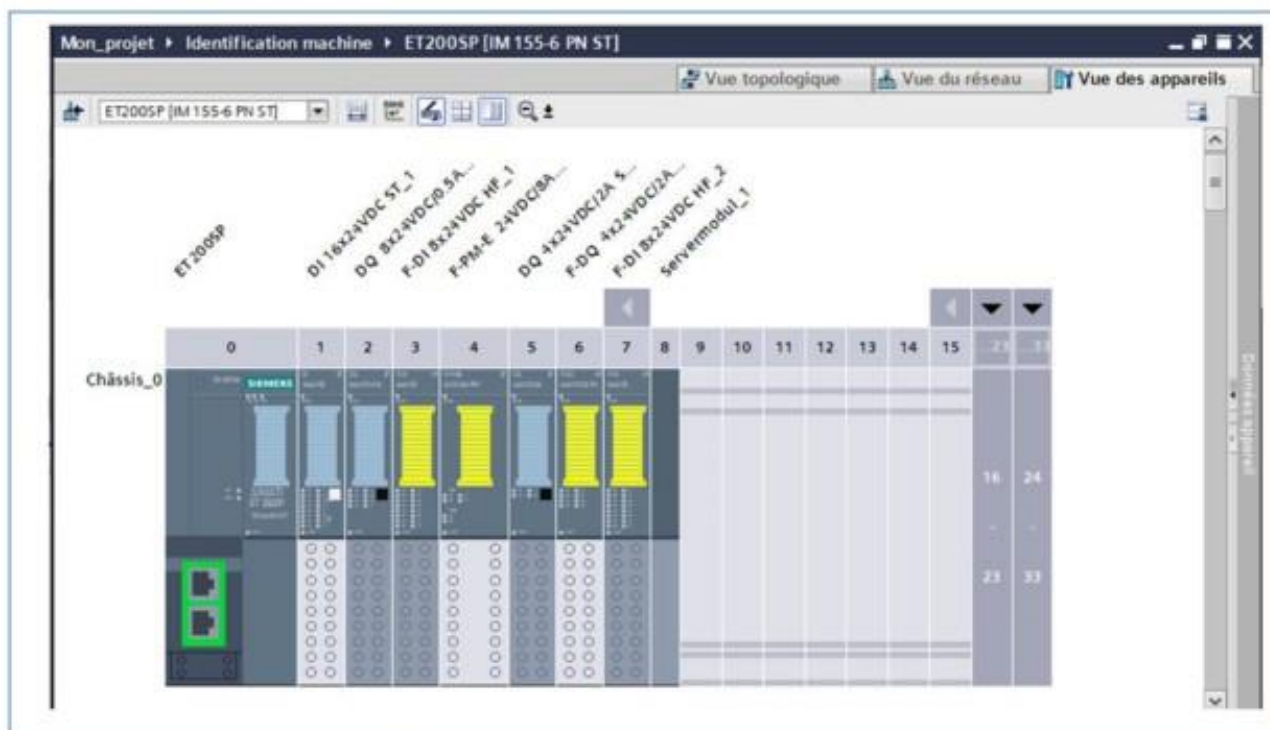
Dans l'exemple représenté ci-dessus, l'option « Aucun accès (protection complète) » est sélectionnée. Sans mot de passe, STEP7 et les appareils IHM (pupitres opérateur) ne peuvent accéder ni en lecture ni en écriture à la CPU. Il est toutefois possible de supprimer les niveaux de protection décrits ci-dessus en entrant les mots de passe correspondants :

- L'entrée du mot de passe (4) permet à un appareil IHM d'accéder à nouveau en lecture et en écriture à la CPU ; l'accès en lecture et en écriture est interdit à STEP7.
- L'entrée du mot de passe (3) permet à un appareil IHM d'accéder à nouveau en lecture et en écriture à la CPU ; l'accès en lecture est autorisé à STEP7, mais pas l'accès en écriture.

Autorisation d'accès par mots de passe

- L'entrée du mot de passe (2) permet à un appareil IHM comme à STEP7 d'accéder en lecture et en écriture au programme standard de la CPU.
- L'entrée du mot de passe (1) permet à un appareil IHM comme à STEP7 d'accéder en lecture et en écriture à la CPU.

4.3. Configurer une station périphérique ET 200SP

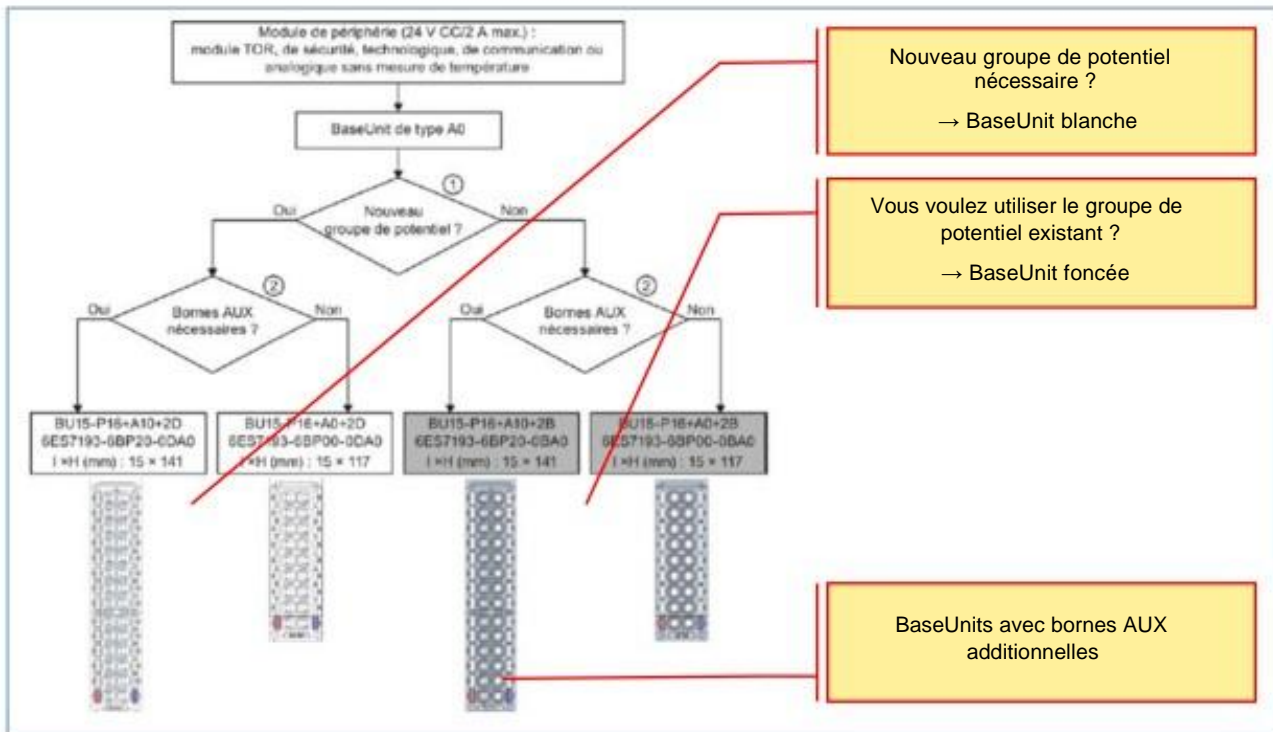


Configurer une station périphérique de sécurité

La configuration des modules de sécurité ET 200SP, ET 200S, ET 200eco, ET 200pro, ET 200iSP et des modules de signaux SM S7-300 s'effectue dans STEP7 de la manière habituelle.

Après avoir inséré la station périphérique de sécurité dans la fenêtre de travail de la « Vue des appareils » ou « Vue du réseau », vous accédez aux boîtes de dialogue pour la configuration en sélectionnant la périphérie concernée et en cliquant sur l'onglet « Propriétés ».

4.3.1. Sélectionner l'unité de base



Sélection de l'unité de base

Il existe différentes unités de base (BaseUnits) pour la station périphérique décentralisée ET 200SP. La BaseUnit définit notamment l'interconnexion avec le processus, le module périphérique enfichable et l'alimentation en tension.

Configuration maximale d'un groupe de potentiel

Le nombre de modules de périphérie utilisables par groupe de potentiel dépend des facteurs suivants :

1. Consommation totale de tous les modules de périphérie exploités sur ce groupe de potentiel
2. Consommation totale de toutes les charges externes connectées à ce groupe de potentiel

La somme du courant total calculé selon les points 1 et 2 ne doit pas dépasser 10 A.

Bornes AUX



Les BaseUnits avec bornes AUX additionnelles (par ex. BU15-P16+A10+2D) permettent de connecter un potentiel supplémentaire (jusqu'à la tension d'alimentation max. du module) que vous appliquez via la barre AUX.

Sélection de la BaseUnit adaptée

Les BaseUnits (BU) sont classées en différents types. Chaque type de BaseUnit se distingue par des caractéristiques adaptées à des modules de périphérie déterminés. Le type de BaseUnit est identifiable aux deux derniers caractères de la référence d'un module de périphérie, par ex.

4 FDO / 6ES7136-6DB00-0CA0 / BaseUnit de type A0.

4.3.2. Unité de base pour le module de puissance et le module à relais

Module de puissance F-PM-E PPM 24VDC/8A	Module à relais F-RQ 1x24VDC/24..230VAC/5A
	
<p>Ouvre un nouveau groupe de potentiel pour la coupure de groupe BaseUnit : BU20-P6+A2+4D Référence : 6ES7193-6BP20-0DC0</p>	<p>BaseUnits spéciales pour F-RQ BaseUnit : BU20-P8+A4+0B Référence : 6ES7193-6BP20-0BF0</p>

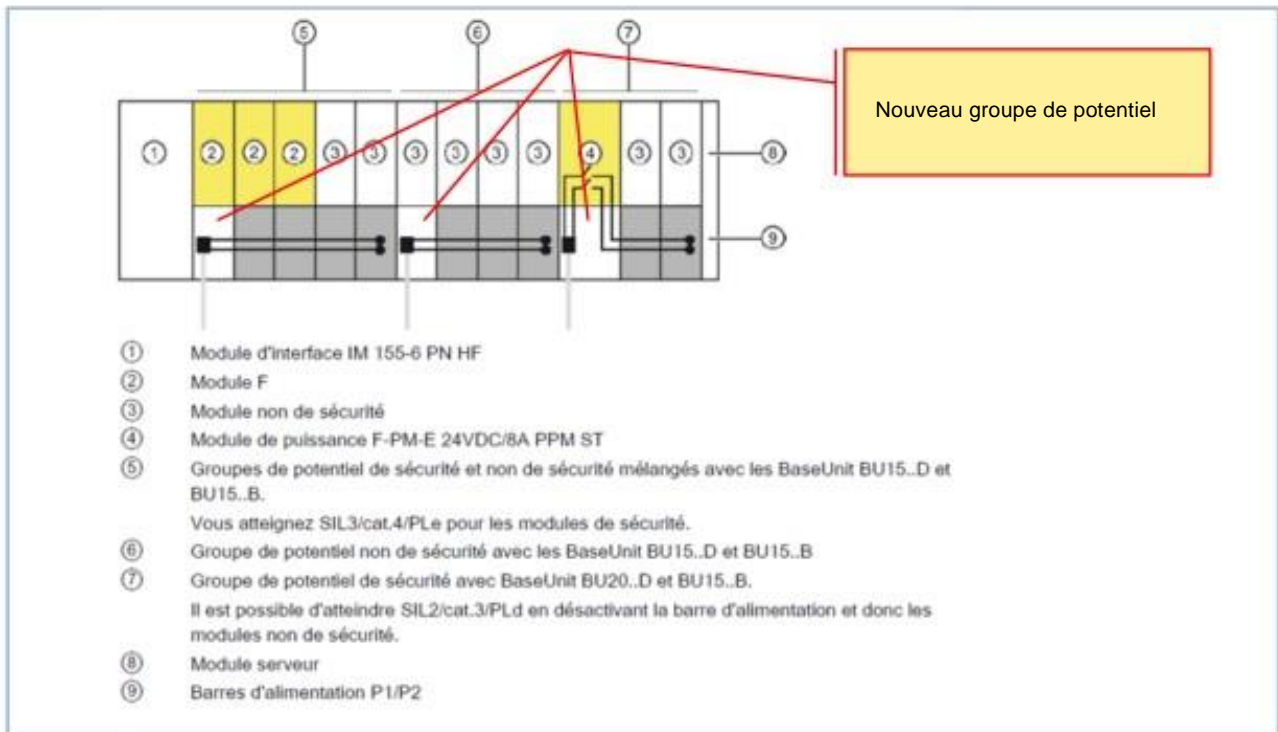
Sélection de l'unité de base

Lors de la mise en service, veillez à ce que le module de puissance ne soit utilisé qu'avec une BaseUnit de type C0.

Remarque

La BaseUnit a été correctement sélectionnée si les deux derniers caractères de la référence/MLFB du module figurent aussi dans la référence/MLFB de la BaseUnit.

4.3.3. ET 200SP avec modules de sécurité et modules standard

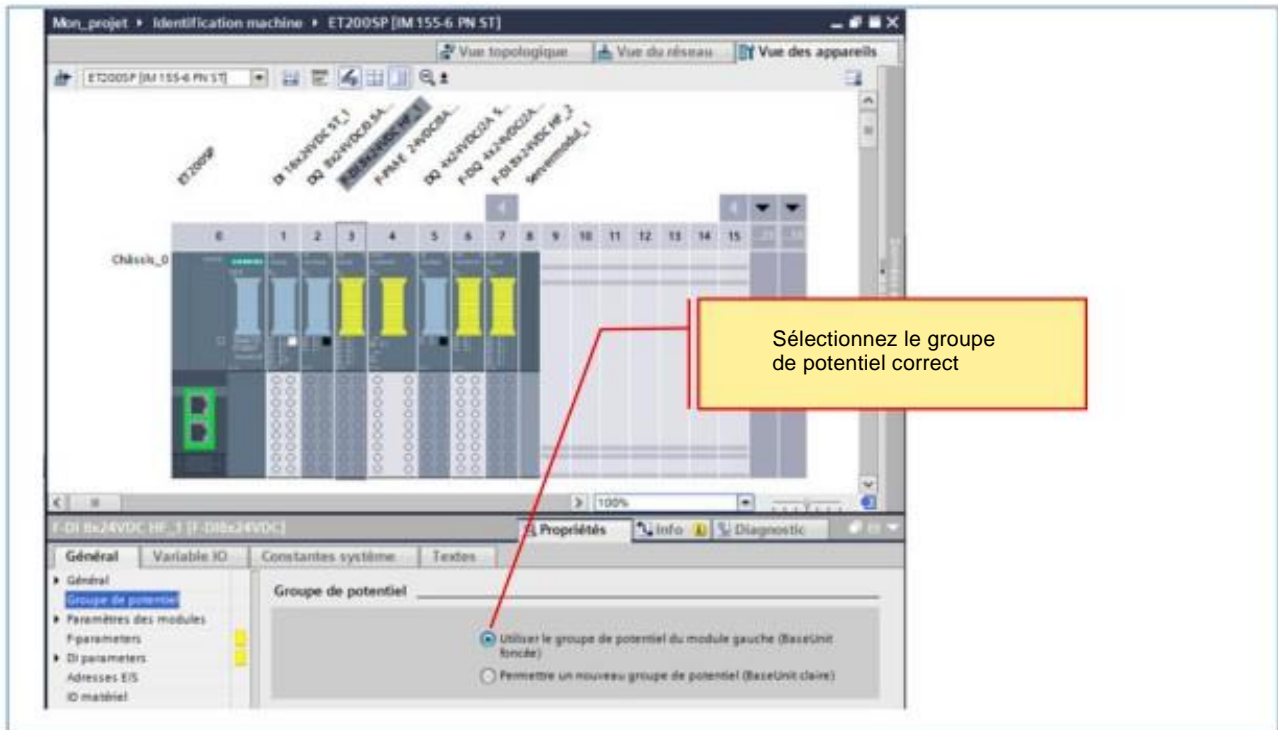


ET 200SP avec modules de sécurité et modules standard

Vous pouvez configurer la station périphérique ET 200SP avec des modules de sécurité et des modules standard. Il n'est en principe pas nécessaire d'exploiter les modules de sécurité et les modules standard dans des groupes de potentiel séparés.

4.3.4. Paramètres de la station périphérique de sécurité

4.3.4.1. Groupe de potentiel



Groupe de potentiel

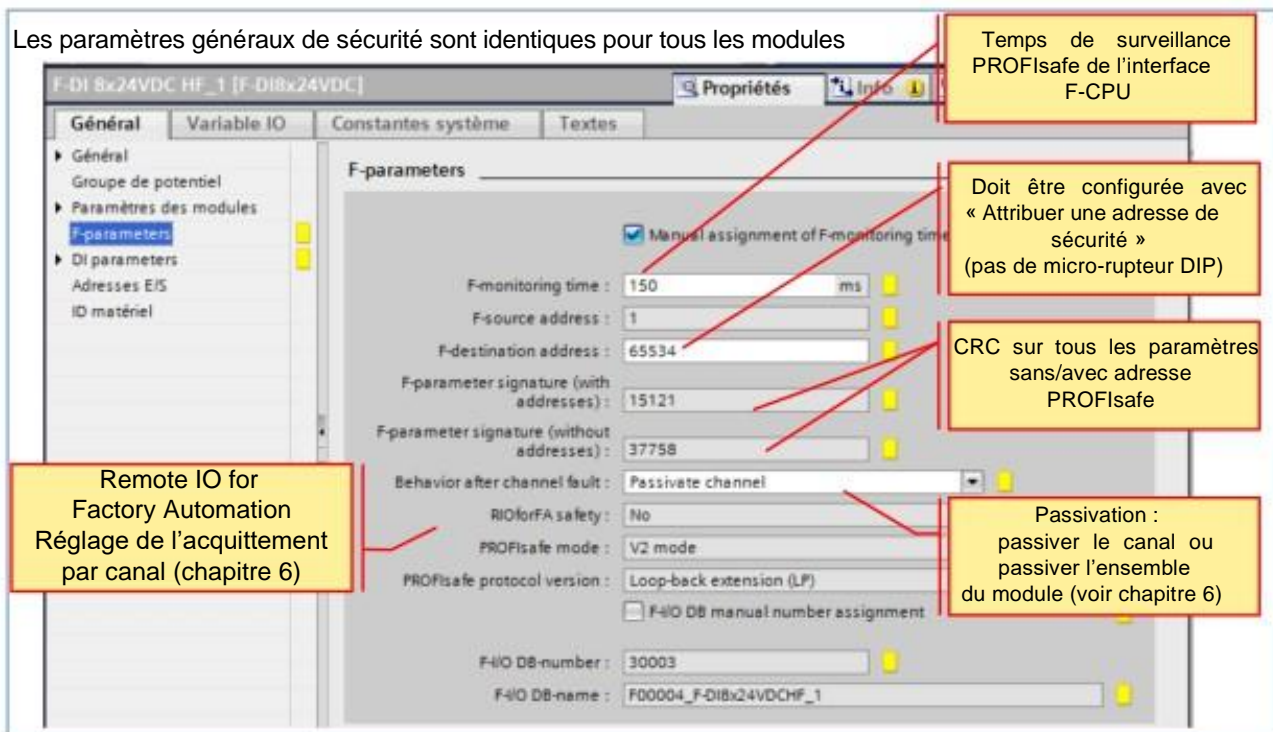
Sur la station périphérique décentralisée ET 200SP, les groupes de potentiel créés dépendent de la disposition des unités de base (BaseUnits).

Pour la formation de groupes de potentiel, la station ET 200SP distingue deux BaseUnits :

- les BaseUnits BU...D (reconnaissables à la boîte à bornes claire et au déverrouillage clair du profilé support) :
 - Ouverture d'un nouveau groupe de potentiel (la barre d'alimentation et la barre AUX sont interrompues à gauche)
 - Tension d'alimentation L+ jusqu'à un courant d'alimentation de 10 A
- BaseUnits BU...B (reconnaissables à la boîte à bornes foncée et au déverrouillage foncé du profilé support) :
 - Prolongement du groupe de potentiel (barre d'alimentation et barre AUX non interrompues) – Prélèvement de la tension d'alimentation L+ pour des composants externes ou
 - Rebouclage avec un courant total maximal de 10 A

4.3.4.2. Paramètres généraux de sécurité

Les paramètres généraux de sécurité sont identiques pour tous les modules



Paramètres généraux de sécurité (F-parameters)

L'onglet « F-parameters » permet de procéder au paramétrage de la communication de sécurité du module avec la CPU F.

Adresses cibles

Il s'agit des adresses PROFIsafe servant à l'identification claire de la source (CPU F) et de la cible (module F). Les adresses PROFIsafe doivent être définies de manière univoque à l'échelle de la station et du réseau. Afin d'éviter un mauvais paramétrage, l'adresse cible est automatiquement attribuée. En cas de modification manuelle de l'adresse cible F, son unicité à l'échelle de la station est automatiquement vérifiée, mais pas son unicité à l'échelle du réseau. C'est à l'utilisateur de s'en assurer par lui-même.

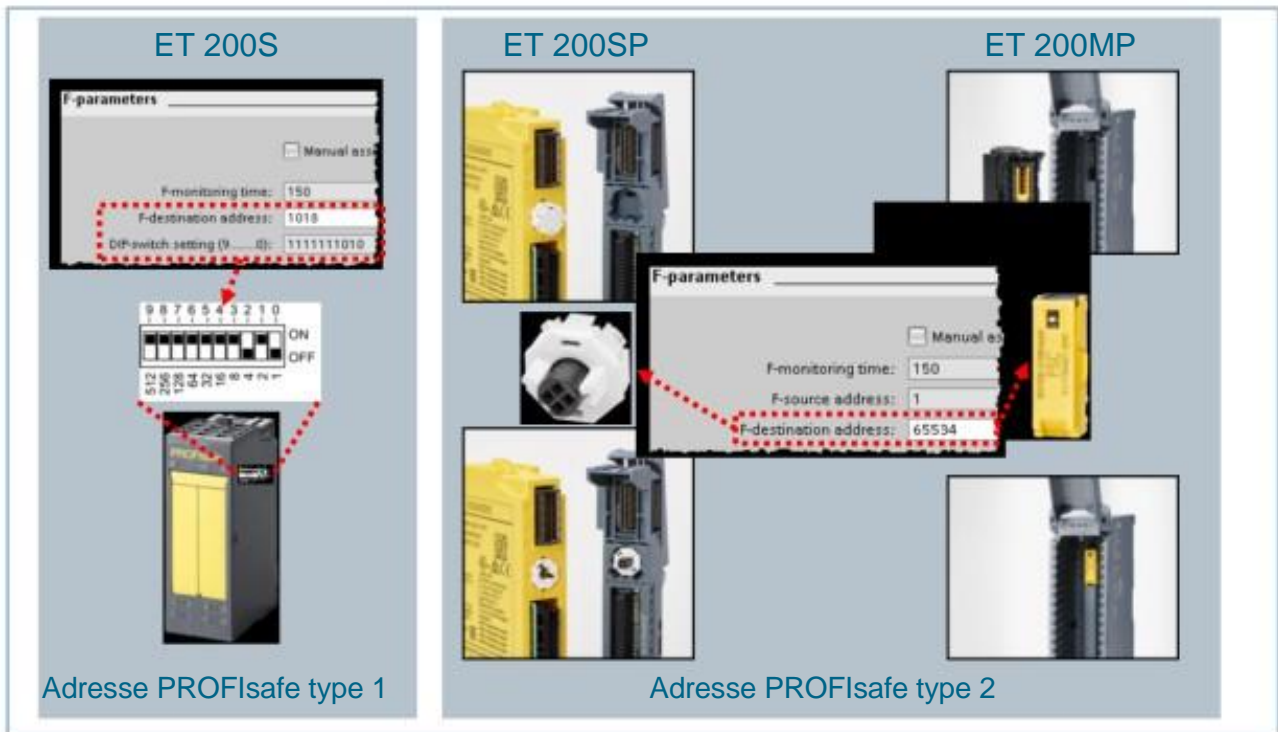
Temps de surveillance F [ms]

Il s'agit du temps de surveillance PROFIsafe pour la communication de sécurité entre la CPU F et la périphérie F. Si la périphérie F ne reçoit aucun télégramme de sécurité valide de la CPU F durant le temps de surveillance paramétré, le module F est passivé et une « erreur de communication » est générée. Le temps de surveillance peut être défini manuellement, de manière spécifique à chaque module, ou de manière centralisée pour tous les modules de sécurité via les paramètres F de la CPU.

Comportement en cas de défaut sur un canal

À partir de S7 Distributed Safety V 5.4, le comportement des modules périphériques de sécurité en cas de défaut sur un canal (par ex. court-circuit, surcharge, erreur de discordance, rupture de fil) est configurable. Si la périphérie de sécurité prend en charge ce paramètre (par ex. pour les modules F ET 200SP, ET 200S), il est possible de définir si le module entier doit être passivé, ou si ce sont les canaux défectueux qui doivent être passivés.

4.3.5. Montage et adressage d'un module de périphérie de sécurité ET200SP/MP



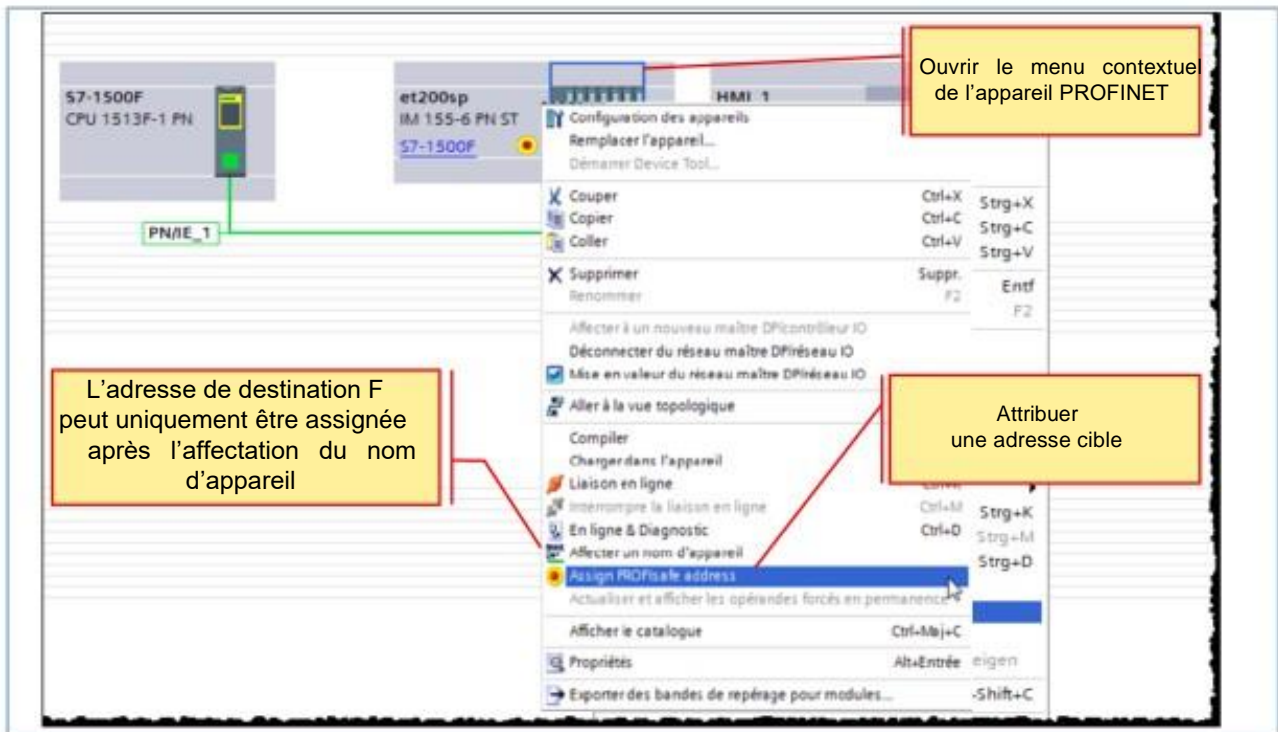
Adresse cible pour les modules de sécurité

L'adresse cible est mémorisée de manière permanente sur l'élément de codage des modules de sécurité ET 200SP. Lors de l'attribution de l'adresse cible, le module doit être alimenté par la tension d'alimentation L+.

Remarque importante concernant le contrôle de configuration :

Avant de pouvoir utiliser le contrôle de configuration avec les modules de sécurité, vous devez affecter l'adresse cible aux modules situés aux emplacements prévus. Les modules de sécurité doivent pour ce faire être enfichés aux différents emplacements configurés. La configuration physique pourra ensuite être différente de celle configurée.

4.3.6. Attribuer une adresse de sécurité



Attribuer une adresse de sécurité

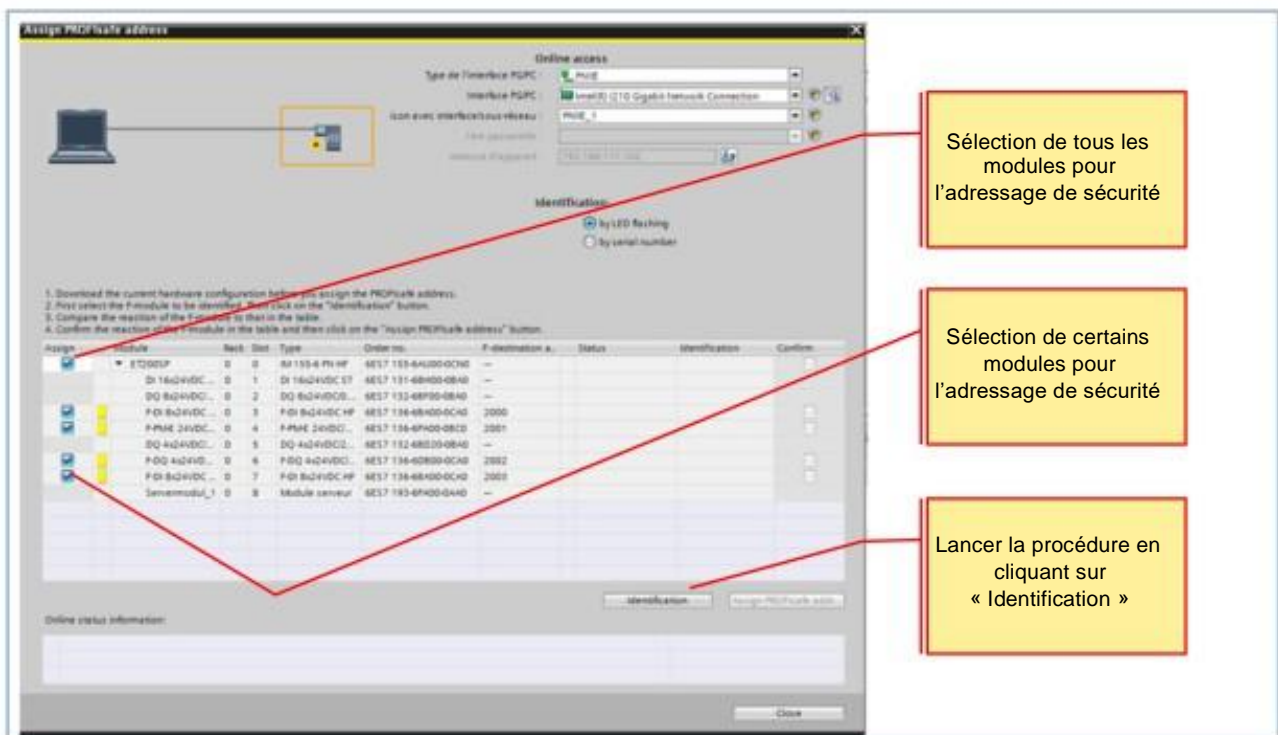
Les modules de sécurité ET 200SP ne possèdent pas de microprocesseur DIP permettant d'attribuer une adresse cible univoque à chaque module. L'adresse PROFIsafe est attribuée directement à partir de STEP 7. L'adresse cible F se paramètre dans la configuration matérielle du module F. L'adresse source correspond, pour les configurations prises en charge, au paramètre « Base pour adresses PROFIsafe » de la CPU F correspondante. Une attribution est également nécessaire dans les cas suivants :

- Enfichage ultérieur d'un module F lors de la première mise en service
- Réparation de l'ET 200SP
- Remplacement de la BaseUnit
- Mise en service d'une machine de série
- Modification de l'adresse cible F
- Modification du paramètre « Base pour adresses PROFIsafe » de la CPU F correspondante (modifie l'adresse source F)

Une nouvelle attribution de l'adresse n'est pas nécessaire dans les cas suivants :

- Mise hors tension/sous tension
- Remplacement d'un module de sécurité (réparation) sans PG/PC
- Modification de la configuration lorsqu'une nouvelle BaseUnit est insérée avant un module F
- Réparation/remplacement du module

4.3.7. Identifier les modules de sécurité



Identifier les modules de sécurité

En cliquant sur le bouton « Identification », vous confirmez l'exactitude des adresses pour la périphérie de sécurité. Lors de la confirmation de la périphérie de sécurité par le clignotement des LED ou par le numéro de série du module d'interface, les conditions suivantes doivent être remplies :

- La station ET 200SP est configurée.
- La configuration a été chargée dans la station ET 200SP.
- La station ET 200SP est accessible en ligne.

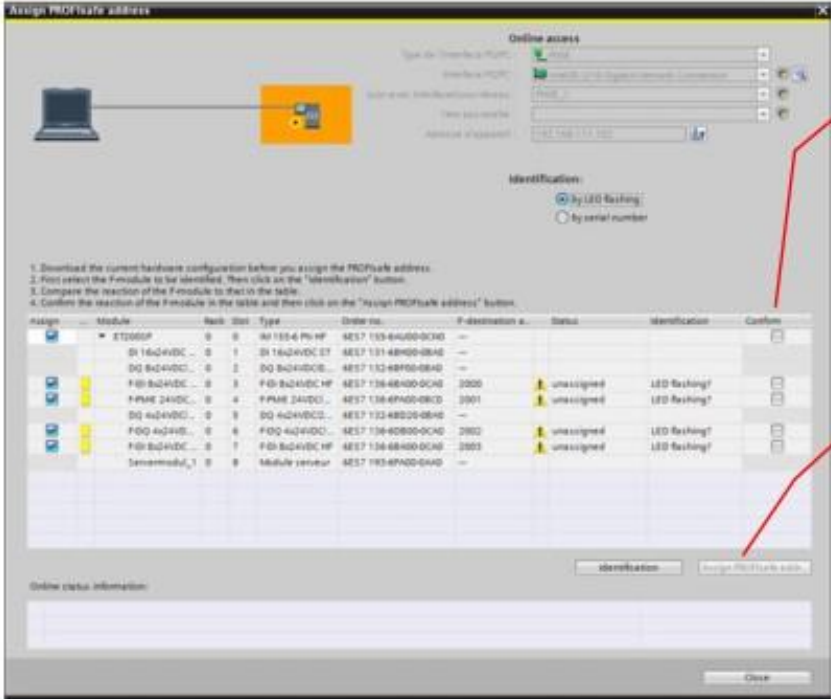
« Identifier par clignotement des LED »

Il s'agit du paramétrage par défaut. Lors de l'identification, les LED DIAG et STATUS des modules à identifier clignotent.

« Identifier par numéro de série »

Si vous n'avez pas les modules de sécurité sous les yeux, vous pouvez les identifier via le numéro de série du module d'interface.

4.3.8. Attribuer une adresse cible



Online access

Type of connection: ☒ PROFIsafe

Connection name: PROFIsafe

Connection ID: 1

Connection password: 1234567890123456

Identification:

☒ By LED flashing

☐ By serial number

1. Download the current hardware configuration before you assign the PROFIsafe address.
 2. First enter the P-number to be identified, then click on the "Identification" button.
 3. Compare the reaction of the P-number to flash in the table.
 4. Confirm the reaction of the P-number in the table and then click on the "Assign PROFIsafe address" button.

Assign	Module	Rank	Slot	Type	Order no.	P-number	Status	Identification	Confirm
<input checked="" type="checkbox"/>	PS 307 5A	0	0	PS 307 5A	6ES7 307-1EA00-0AA0	---			
<input checked="" type="checkbox"/>	DI 16xDC24VDC	0	1	DI 16xDC24VDC	6ES7 321-1BH02-0AA0	---			
<input checked="" type="checkbox"/>	DO 16xDC24VDC	0	2	DO 16xDC24VDC	6ES7 322-1BH01-0AA0	---			
<input checked="" type="checkbox"/>	AI 5/AO 1	0	3	AI 5/AO 1	6ES7 331-7KF02-0AB0	2000	unassigned	LED flashing?	
<input checked="" type="checkbox"/>	PA 16xDC24VDC	0	4	PA 16xDC24VDC	6ES7 344-1EX30-0AB0	2001	unassigned	LED flashing?	
<input checked="" type="checkbox"/>	DO 16xDC24VDC	0	5	DO 16xDC24VDC	6ES7 322-1BH01-0AA0	---			
<input checked="" type="checkbox"/>	AI 5/AO 1	0	6	AI 5/AO 1	6ES7 331-7KF02-0AB0	2002	unassigned	LED flashing?	
<input checked="" type="checkbox"/>	DO 16xDC24VDC	0	7	DO 16xDC24VDC	6ES7 322-1BH01-0AA0	2003	unassigned	LED flashing?	
<input checked="" type="checkbox"/>	Power supply	0	8	Power supply	6ES7 307-1EA00-0AA0	---			

Online status information:

Identification

Assign PROFIsafe address

Close

L'utilisateur doit confirmer que les LED des modules sélectionnés clignotent.

Lorsque l'utilisateur confirme sur l'appareil de périphérie, tous les modules de l'appareil sont confirmés.

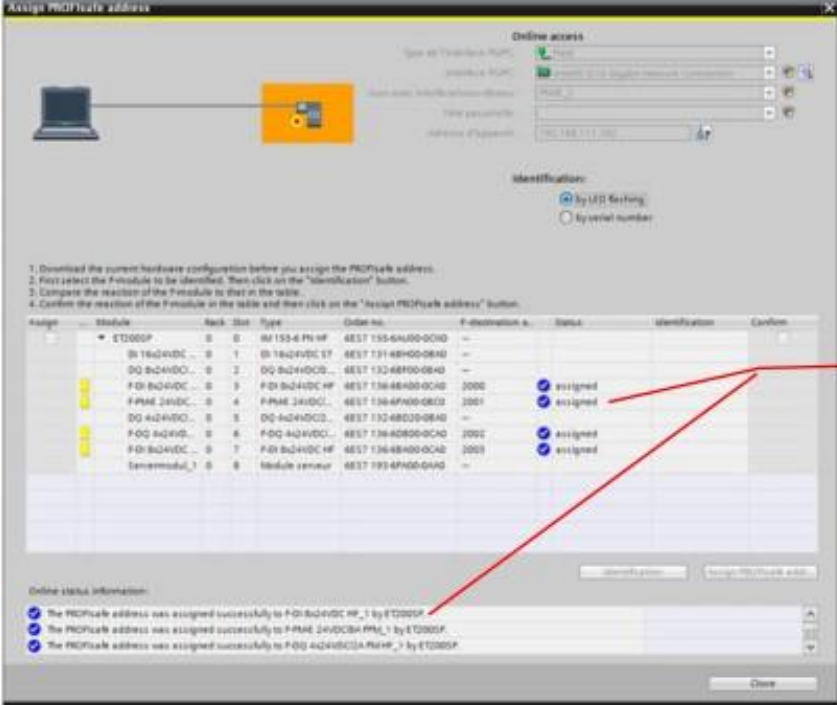
Le bouton « Assign PROFIsafe address » n'est activé que si tous les modules sélectionnés dans cet appareil sont confirmés.

L'utilisateur attribue l'adresse de sécurité en cliquant sur ce bouton.

Attribuer une adresse cible

Pour attribuer l'adresse cible, vous devez confirmer la boîte de dialogue « Confirmer l'attribution » dans un délai de 60 secondes.

4.3.9. État de l'adresse cible



Assign PROFsafe address

Online access

Identification:

1. Download the current hardware configuration before you assign the PROFsafe address.
 2. First select the P-module to be identified, then click on the "Identification" button.
 3. Compare the reaction of the P-module to that in the table.
 4. Confirm the reaction of the P-module in the table and then click on the "Assign PROFsafe address" button.

Assign	Module	Rack	Slot	Type	Order no.	P-destination s.	Status	Identification	Confirm
	ET200SP	0	0	AI 15x4 Pt HF	6ES7 155-6A00-0000	---			
	DI 16x4xDC ...	0	1	DI 16x4xDC ST	6ES7 131-6B00-0000	---			
	DO 8x4xDC ...	0	2	DO 8x4xDC S...	6ES7 132-6B00-0000	---			
	FDI 8x4xDC ...	0	3	FDI 8x4xDC HF	6ES7 136-6B00-0000	2000	assigned		
	FPAE 2x4xDC ...	0	4	FPAE 2x4xDC...	6ES7 136-6B00-0000	2001	assigned		
	DO 4x4xDC ...	0	5	DO 4x4xDC...	6ES7 132-6B00-0000	---			
	FDQ 4x4xDC ...	0	6	FDQ 4x4xDC...	6ES7 136-6B00-0000	2002	assigned		
	FDI 8x4xDC ...	0	7	FDI 8x4xDC HF	6ES7 136-6B00-0000	2003	assigned		
	Servermodul 1	0	8	Module server	6ES7 193-6B00-0000	---			

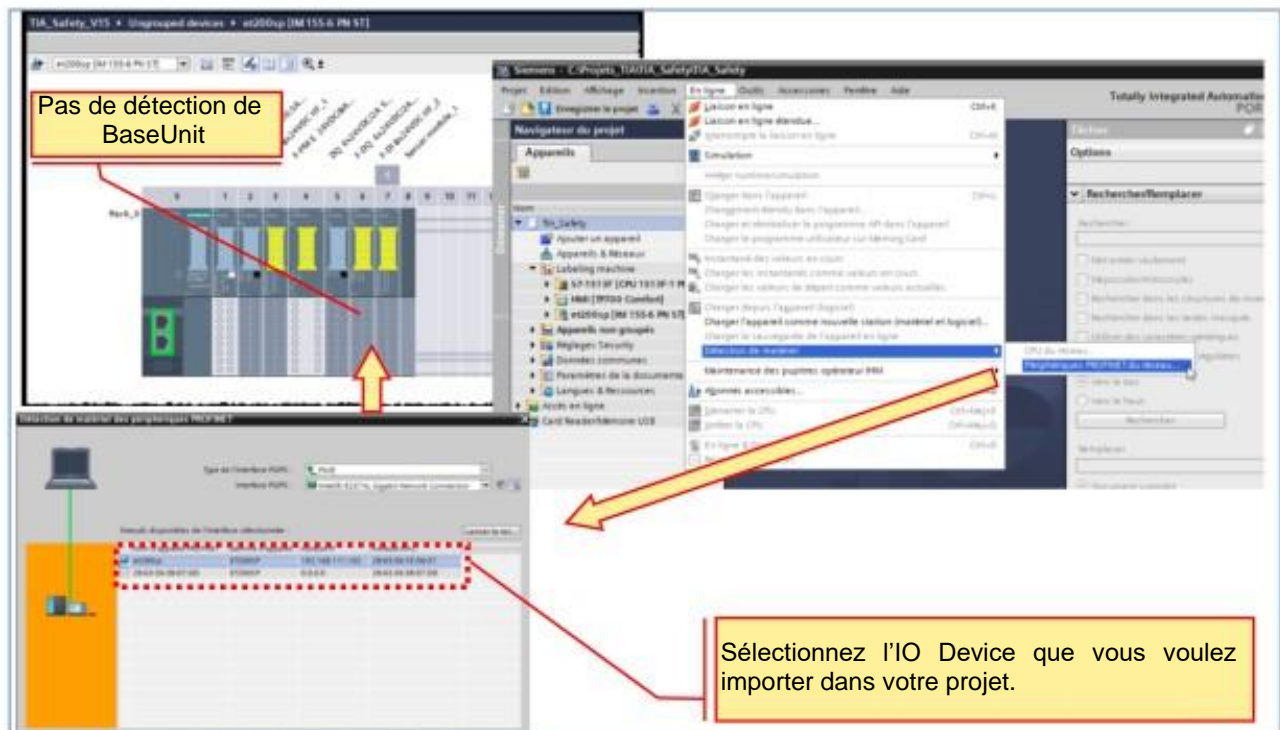
Online status information:

- The PROFsafe address was assigned successfully to FDI 8x4xDC HF_1 by ET200SP
- The PROFsafe address was assigned successfully to FPAE 2x4xDC FPAE_1 by ET200SP
- The PROFsafe address was assigned successfully to FDQ 4x4xDC FPAE_1 by ET200SP

Close

Si l'adresse de sécurité a été attribuée avec succès, l'état OK et un message s'affichent dans les informations d'état à l'attention de l'utilisateur.

4.4. Configurez un IO device avec la détection de matériel



Vous avez la possibilité de détecter un module de périphérie d'E/S et de l'importer dans votre projet grâce à la fonction « Détection de matériel ». Un périphérique détecté peut être importé dans votre projet STEP7 avec tous les modules et sous-modules.

Pré-requis

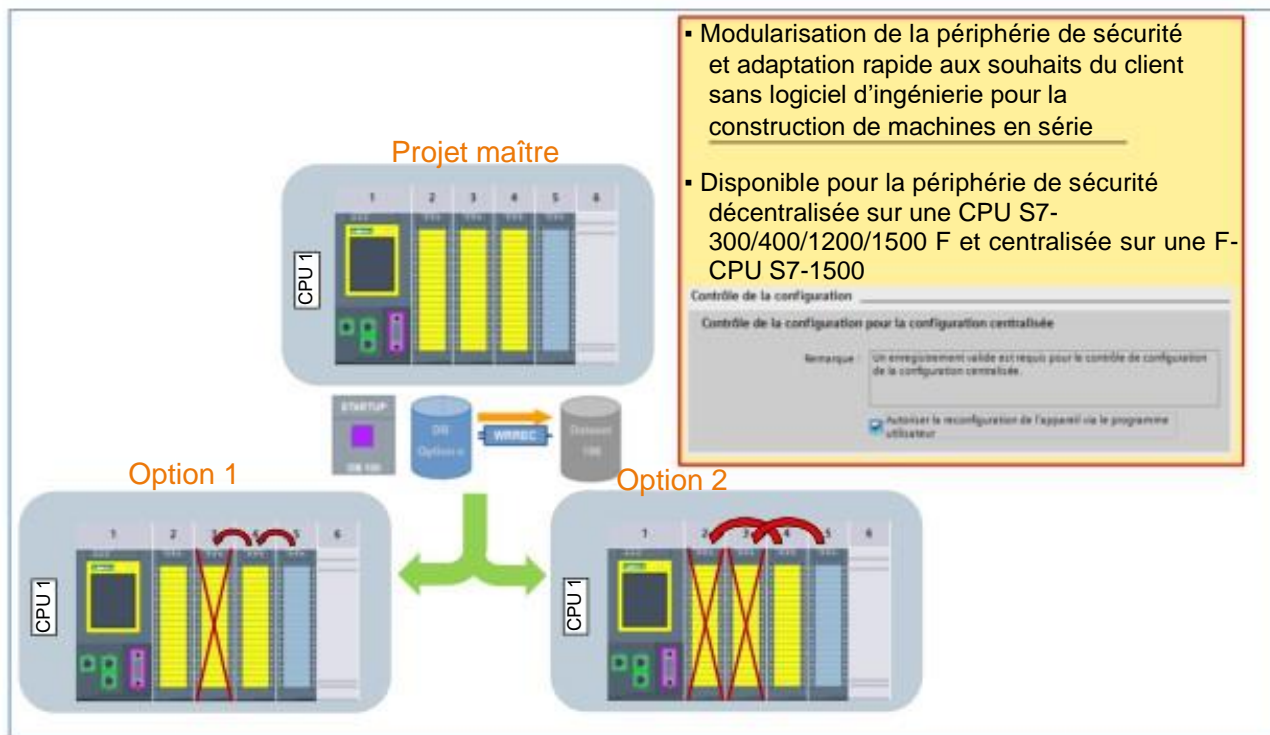
- STEP 7 (TIA Portal) à partir de V15
- L'accès au module doit être techniquement réalisable

Résultat de la détection de matériel

Un module d'E/S configuré par détection de matériel se comporte comme suit :

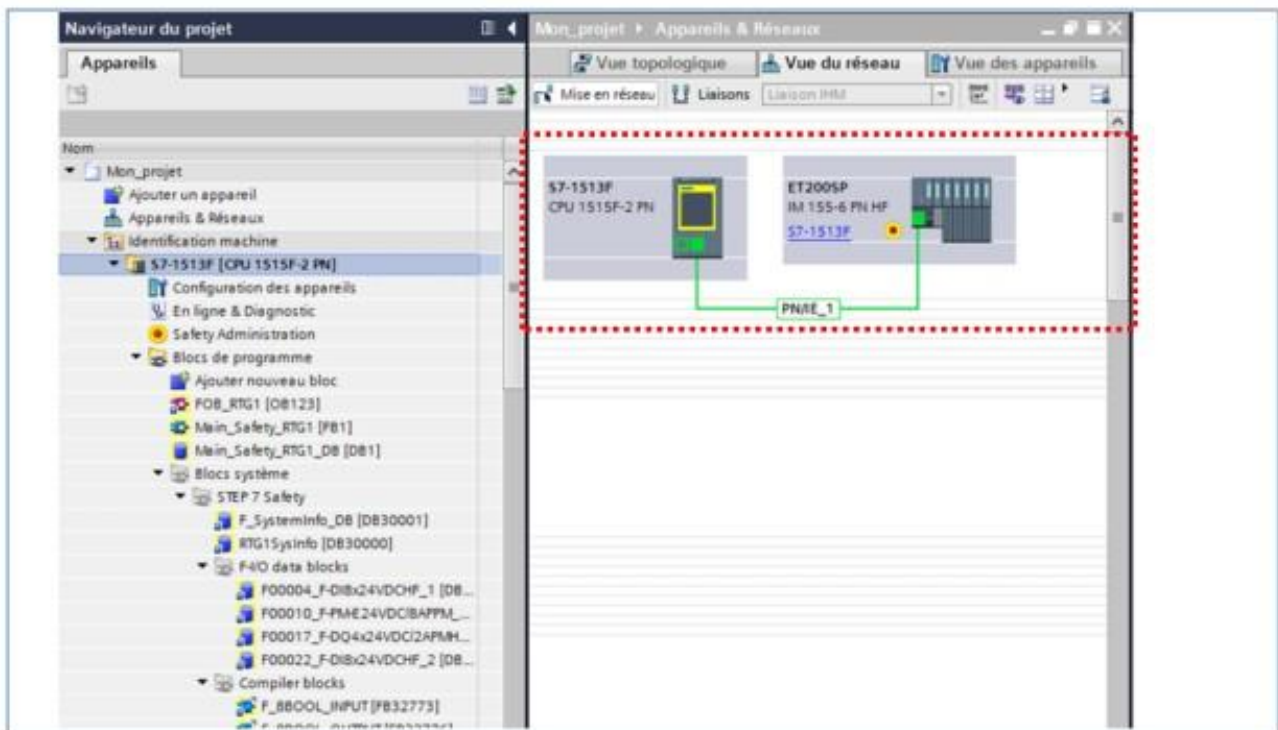
- Les modules configurés via la « détection de matériel » sont configurés comme s'ils avaient été insérés à partir du catalogue.
- STEP 7 intègre l'adresse MAC du périphérique d'E/S détecté au projet.
- Paramètres IP :
 - Si le périphérique d'E/S détecté possède déjà une adresse IP, STEP 7 applique l'adresse IP au projet.
 - Si le périphérique d'E/S détecté n'a pas d'adresse IP, STEP 7 attribue automatiquement une adresse IP au projet.
- Noms des modules PROFINET:
 - Si le périphérique d'E/S détecté possède déjà un nom de périphérique PROFINET, STEP 7 applique le nom de périphérique PROFINET au projet.
 - Si le périphérique d'E/S détecté ne possède pas de nom de périphérique PROFINET, STEP 7 attribue automatiquement un nom de périphérique PROFINET dans le projet.
- Les périphériques d'E/S configurés via la « Détection de matériel » ne sont ni affectés à un sous-réseau IP ni à un contrôleur.

4.4.1. Contrôle de configuration (traitement des options) pour la station périphérique de sécurité



Pour le contrôle de configuration (traitement des options) avec des modules I/O F procédez comme avec les modules I/O standards. Des informations détaillées sont disponibles dans l'aide de Step7 sous « Contrôle de configuration (traitement des options) ». Vous trouvez également un exemple d'application dans l'article ID : 54110126).

4.5. Énoncé : Créer un projet et une station matérielle



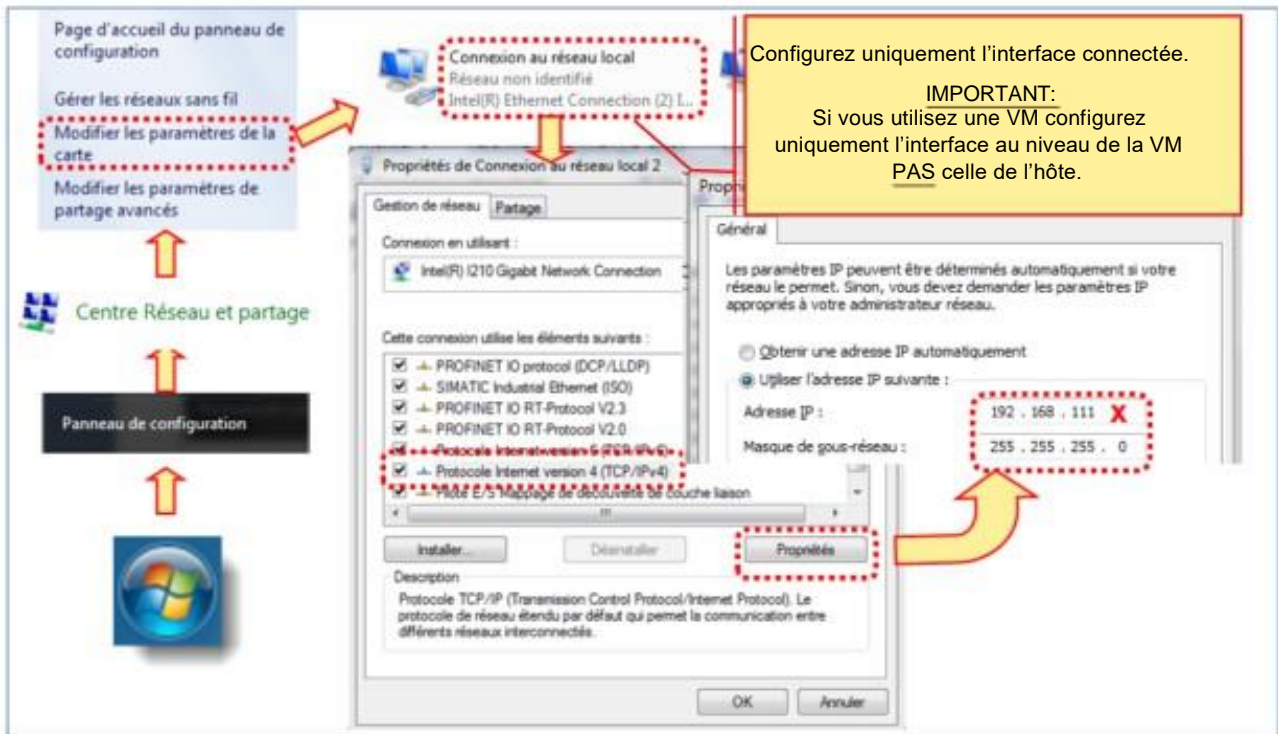
Enoncé

Vous devez créer la configuration matérielle pour la CPU et l'ET 200SP dans un nouveau projet.

Marche à suivre

Ce que vous devez faire sera expliqué dans les pages suivantes.

4.5.1. Exercice 1 : Définir l'adresse IP de la PG



Énoncé et marche à suivre :

1. Connectez un câble Ethernet à l'interface de la PG et à la connexion « P1 ou P2 » de la station de travail.
2. Attribuez l'adresse IP 192.168.111.X et le masque de sous réseau 255.255.255.0 à cette interface. Procédez comme indiqué dans la vue.

Note!

Si vous utilisez une VM, définissez uniquement l'interface dans la VM. Ne changer rien à l'interface de l'hôte!

4.5.2. Exercice 2 : Effacer la carte mémoire SIMATIC (SMC)



Énoncé

Pour effacer complètement la CPU, vous devez aussi effacer la carte mémoire SIMATIC (SMC) de la CPU.

Marche à suivre


1. Insérez la carte mémoire SIMATIC dans le lecteur de carte de la PG, contacts orientés vers le haut. S'il s'agit d'une console de programmation SIMATIC Field PG de type MX, celui-ci dispose de deux lecteurs de cartes. Utilisez le lecteur de gauche pour la carte mémoire SIMATIC.
2. Effacez la carte mémoire SIMATIC. Une boîte de dialogue Windows s'ouvre pour l'ouverture de l'explorateur Windows. Si vous travaillez avec une VM, la SMC n'est détecté que dans l'hôte et NON dans la VM. Ouvrez le dossier. Selon le paramétrage de l'explorateur Windows, les fichiers cachés sont visibles ou masqués.

Attention !

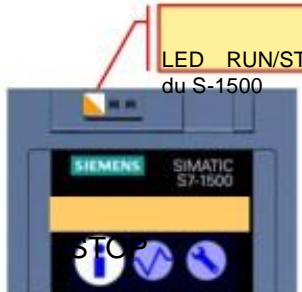
Si les fichiers cachés sont visibles, ils ne doivent en aucun cas être supprimés. Supprimez le répertoire SIMATIC et le fichier de tâches (JOB).

3. **NE REMETTEZ PAS** la carte mémoire SIMATIC dans la CPU. Fermez la fenêtre de l'explorateur Windows et retirez la carte mémoire de la PG après avoir activé la fonction Windows « Retirer le périphérique en toute sécurité ! ».

4.5.3. Exercice 3 : Réinitialiser la CPU et effectuer un redémarrage



1. Placez le sélecteur de mode sur STOP
2. Maintenez le sélecteur de mode sur MRES jusqu'à ce que la LED RUN/STOP clignote 2x lentement
puis relâchez le sélecteur de mode
↓ dans les 3 s !!!
3. Maintenez le sélecteur de mode sur MRES jusqu'à ce que la LED RUN/STOP commence à clignoter rapidement
puis relâchez le sélecteur de mode et attendez que la CPU ait terminé la réinitialisation
4. Réinsérez la carte mémoire et placez le sélecteur de mode sur RUN. La CPU redémarre.



LED RUN/STOP
du S-1500

Résultat :

avec carte mémoire enfichée → effacement général

sans carte mémoire enfichée → réinitialisation aux paramètres usine

Énoncé

Après avoir effacé la carte mémoire SIMATIC de la CPU lors du précédent exercice, vous devez à présent réinitialiser la CPU aux paramètres usine. Vous devez pour ce faire effectuer un effacement général sans carte mémoire SIMATIC.

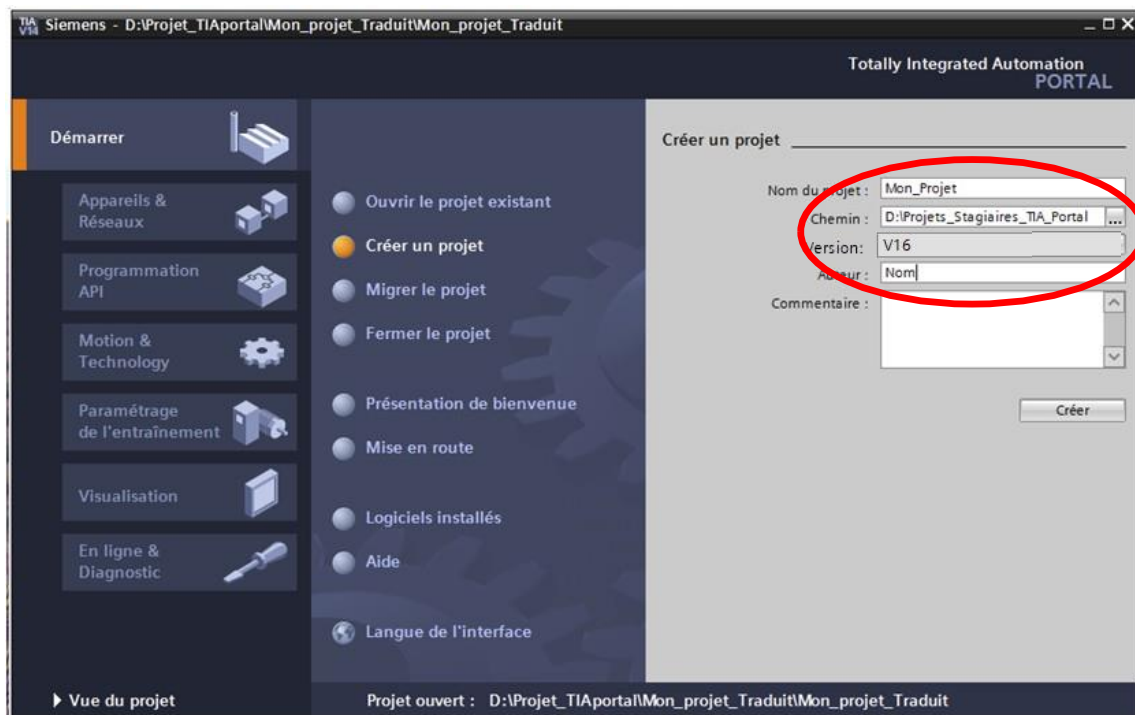
Marche à suivre

1. Effectuez directement l'effacement général sur la CPU selon les étapes indiquées dans la figure.
2. Redémarrez la CPU en faisant passer le sélecteur de mode de STOP à RUN.

Résultat :

- La CPU reste à l'état STOP, car aucun programme utilisateur n'est chargé.
- Les modules périphériques signalent par un clignotement vert qu'ils ne sont pas paramétrés.

4.5.4. Exercice 4 : Créer un nouveau projet



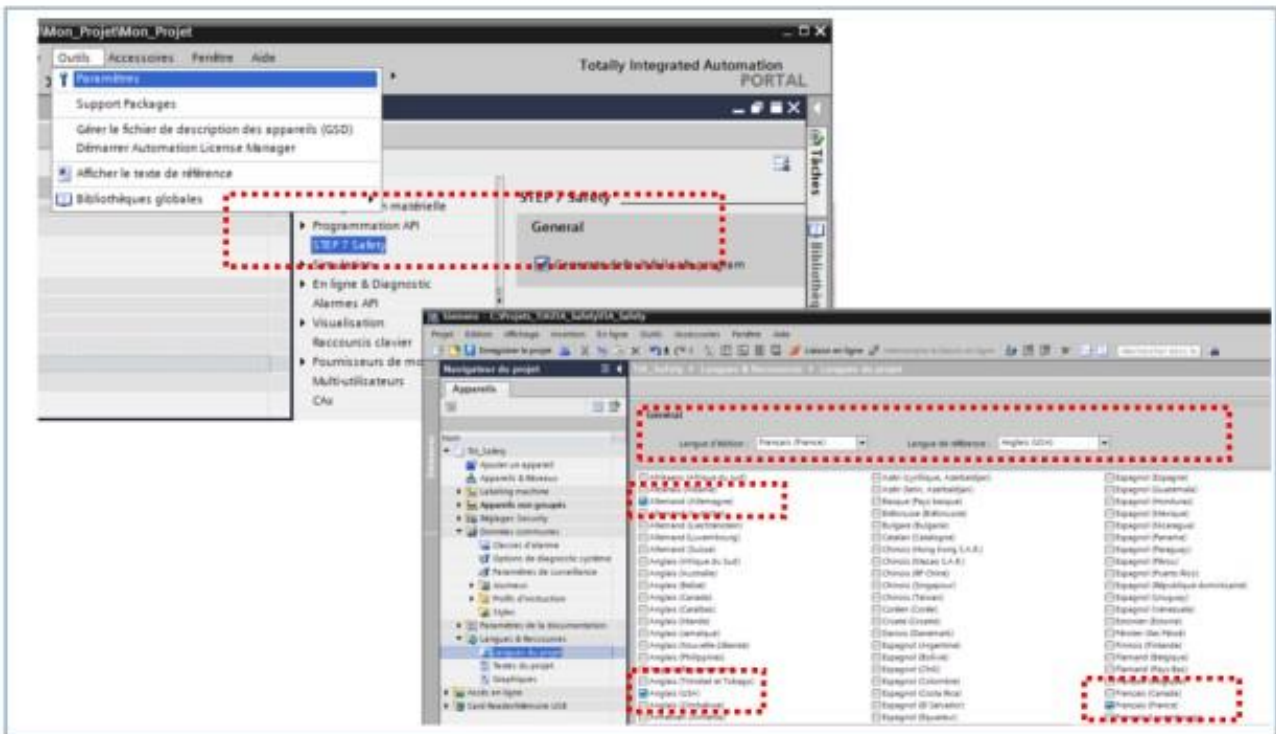
Énoncé

Créez un nouveau projet TIA Portal.

Marche à suivre

1. Ouvrez le TIA Portal.
2. Créez un nouveau projet nommé « Mon_Projet » dans le dossier D:\Projets_Stagiaires_TIA_Portal.

4.5.5. Exercice 5 : Vérifier les paramètres du projet



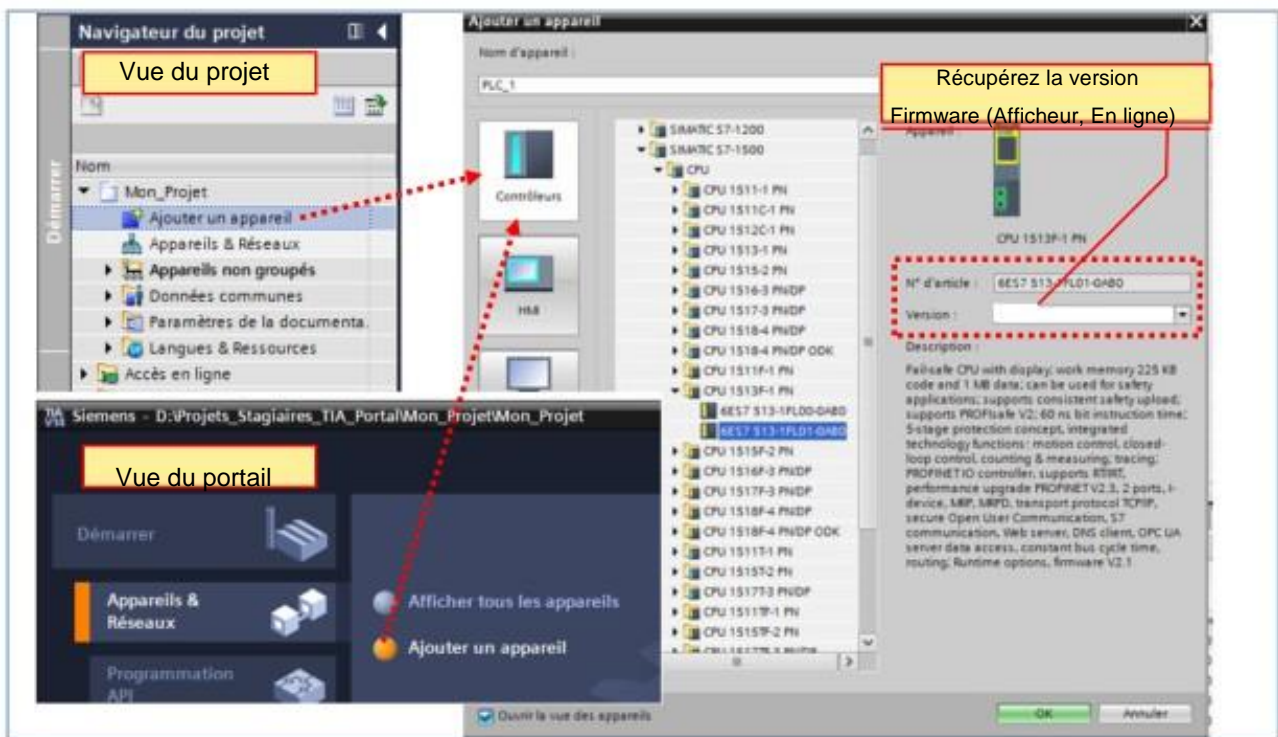
Énoncé

Vérifiez les paramétrages du projet pour STEP7 Safety.

Marche à suivre

1. Allez dans les propriétés du projet relatives à la sécurité.
« Outils » -> « Paramètres » -> « STEP 7 Safety ».
2. Activez « Generate default fail-safe program ».
3. Ouvrez les réglages des langues du projet.
« Navigateur de projet » -> « Langues & Ressources » -> « Langues du projet »
4. Activez Anglais (USA), t Français (France) et Allemand.
5. Retenez Français comme langue d'édition et Anglais comme langue de référence.
6. Enregistrez votre projet

4.5.6. Exercice 6 : Créer une station S7-1500F



Énoncé

Créez une nouvelle CPU S7-1513- F en assurant que la version de firmware corresponde à celle de votre automate de travail.

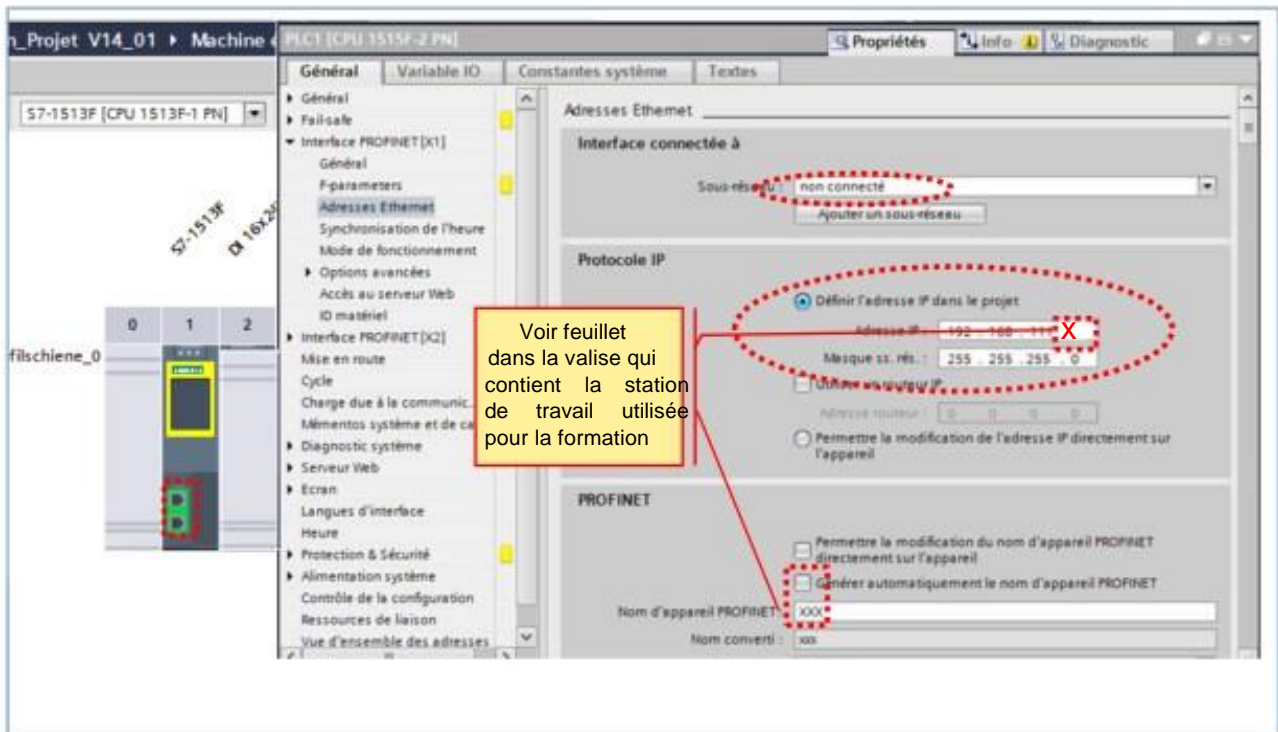
Marche à suivre

1. Récupérez la version du Firmware de votre CPU. Vous pouvez y accéder directement via l'afficheur de la CPU ou via la fonction En ligne du TIA Portal.

Note : Si vous voulez récupérer la version du Firmware via la fonction En ligne du TIA Portal, la CPU nécessite l'affectation d'une adresse IP !

2. Activez l'option « Ajouter un appareil ».
3. Sélectionnez la CPU et le firmware correspondant à votre CPU.

4.5.7. Exercice 7 : Propriétés de la CPU - Adresse IP et nom PROFINET



Énoncé

Attribuez un nom PROFINET et une adresse IP à la CPU.

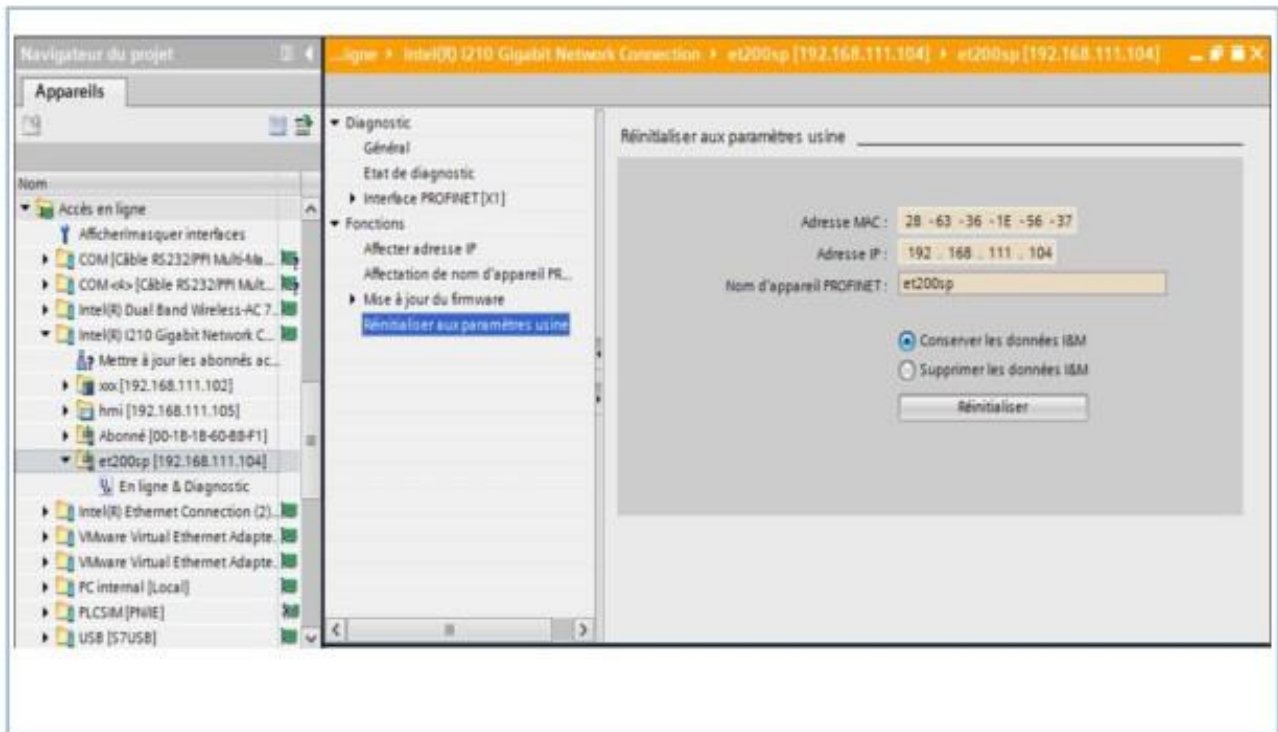
Marche à suivre

1. Allez dans la Vue du projet.
2. Double-cliquez sur la « Configuration d'appareils » de la CPU.
3. Sélectionnez la CPU dans la Vue des appareils.
4. Ouvrez l'onglet « Interface PROFINET » et saisissez l'adresse IP, le masque de sous-réseau et le nom d'appareil figurant sur le feuillet joint à la valise.

Remarque concernant le nom d'appareil :

Le nom d'appareil peut aussi être généré automatiquement. Le nom de l'appareil PROFINET est alors repris du nom de la CPU dans l'onglet « Général ».

4.5.8. Exercice 8 : ET 200SP - Réinitialiser aux paramètres usine



Énoncé

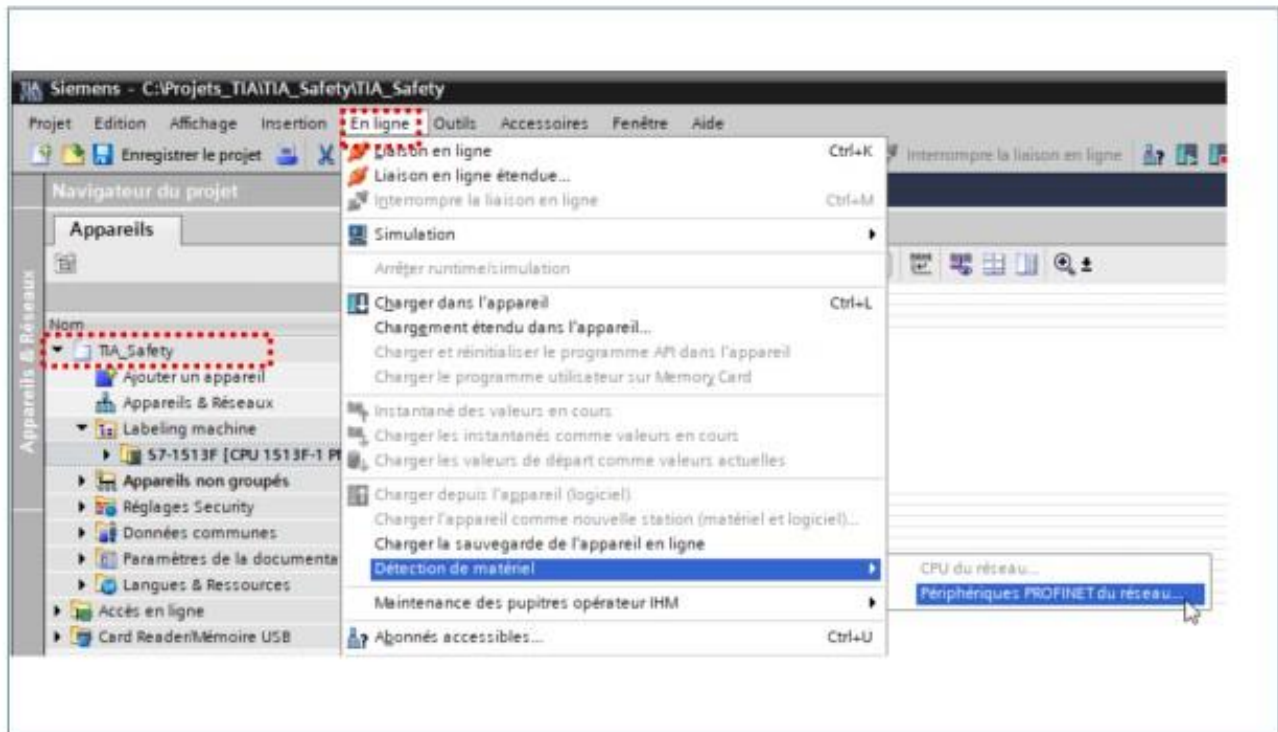
Tous les paramètres antérieurs (adresse IP, masque de sous-réseau et nom PROFINET) du module d'interface et la carte mémoire de la station ET 200SP doivent être effacés par une « réinitialisation aux paramètres usine ». Dans les exercices suivants, vous transférez ensuite vos propres paramètres dans la station ET 200SP

Marche à suivre

1. Ouvrez « Accès en ligne » et sélectionnez l'interface connectée.
2. Double-cliquez sur « Actualiser les abonnés accessibles » et attendez que la liste soit complète.
3. Ouvrez l'ET 200SP et double-cliquez sur la fonction « En ligne & Diagnostic ».
4. Ouvrez l'onglet « Fonctions » dans la fenêtre « En ligne & Diagnostic ».
5. Activez « Réinitialiser aux paramètres usine » et validez.
6. Fermez la fenêtre « En ligne & Diagnostic ».
7. Vérifiez que la réinitialisation a été réalisée avec succès dans la fenêtre d'inspection sous « Info > Général ». Sous « Abonnés accessibles », vous trouverez également l'ET 200SP sans adresse IP et sans nom d'appareil.

Laissez toutes les fenêtres ouvertes pour l'exercice suivant.

4.5.9. Exercice 9 : Détection de l'ET 200SP



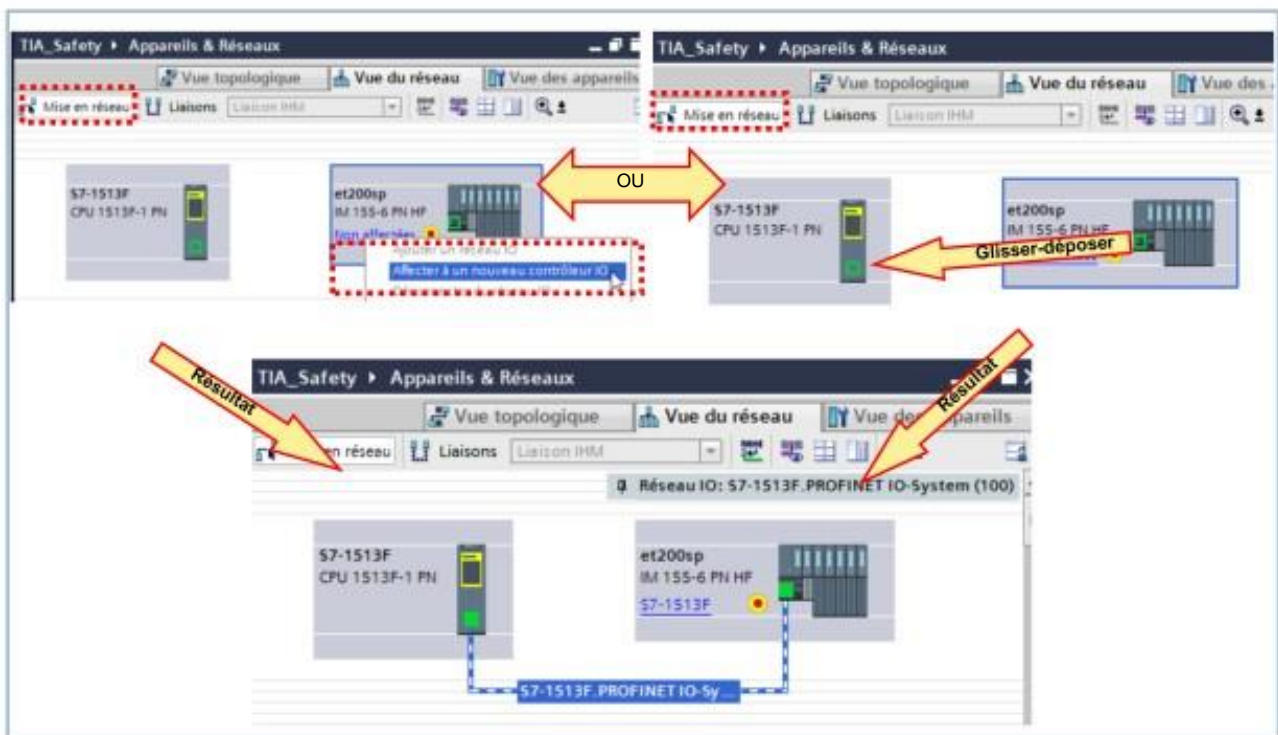
Enoncé

Vous allez récupérer la station ET 200SP dans votre projet.

Marche à suivre

1. Sélectionnez votre projet.
2. Démarrez la détection du matériel pour les périphériques PROFINET.
« En ligne -> Détection de matériel -> Périphériques PROFINET »
3. Dans le dialogue, recherchez la station ET 200SP sur le réseau. Pour ce faire, sélectionnez l'interface PG/PC utilisée et démarrez la recherche.
4. Retenez la station ET 200SP et ajoutez l'appareil.

4.5.10. Exercice 10 : Mettre l'ET 200SP en réseau avec la CPU



Énoncé

Après avoir ajouté la station ET200SP, vous devez l'affecter à un contrôleur ou la mettre en réseau avec une CPU. Seule cette affectation permet de coordonner ou de surveiller les adresses d'E/S des contrôleurs et des périphériques d'E/S lorsque plusieurs CPU sont connectées au réseau.

Marche à suivre

1. Sélectionnez la Vue du réseau dans l'éditeur « Appareils & Réseaux », puis l'onglet « Mise en réseau ».
2. Mettez en réseau l'ET 200SP avec la CPU en connectant l'interface Ethernet de l'ET 200SP à l'interface Ethernet de la CPU par glisser-déposer (vue à droite) ou en l'affectant directement à la CPU (vue à gauche).

4.5.11. Exercice 11 : Adaptez la configuration de l'ET 200SP

Adresses I/O à saisir

2...3	2
4...9	4...7
10...16	10...14
	3
17...21	17...21
22...27	22...25

Sélectionnez la BaseUnit

Vue d'ensemble des appareils

Module	Chassis	Emplacement	Adresse I	Adresse Q	Type	Numéro de article	Firmware
et200sp	0	0			IM 155-6 PN HF	6ES7 155-6A00-0CND	V3.3
Interface PROFINET	0	0 X1			Interface PROFINET		
DI 16x24VDC ST_1	0	1	2...3		DI 16x24VDC ST	6ES7 131-6BH00-0BA0	V1.0
DQ 8x24VDC/0.5A ST_1	0	2		2	DQ 8x24VDC/0.5A ST	6ES7 132-6BH00-0BA0	V1.1
FOI 8x24VDC HF_1	0	3	4...9	4...7	FOI 8x24VDC HF	6ES7 136-6BA00-0CA0	V1.0
FPME 24VDC/0.5A PM ST_1	0	4	10...16	10...14	FPME 24VDC/0.5A PM ST	6ES7 136-6PA00-0BC0	V2.0
DQ 4x24VDC/2A ST_1	0	5		3	DQ 4x24VDC/2A ST	6ES7 132-6BD00-0BA0	V1.1
FOI 4x24VDC/2A PM HF_1	0	6	17...21	17...21	FOI 4x24VDC/2A PM HF	6ES7 136-6DB00-0CA0	V1.0
FOI 8x24VDC HF_2	0	7	22...27	22...25	FOI 8x24VDC HF	6ES7 136-6BA00-0CA0	V1.0
Module serveur_1	0	8			Module serveur	6ES7 193-6PA00-0AA0	V1.1

Énoncé

La configuration de l'ET200SP du projet hors ligne doit correspondre exactement à la configuration de votre appareil de travail. Vous devez veiller en particulier à l'exactitude des références et des versions des modules.

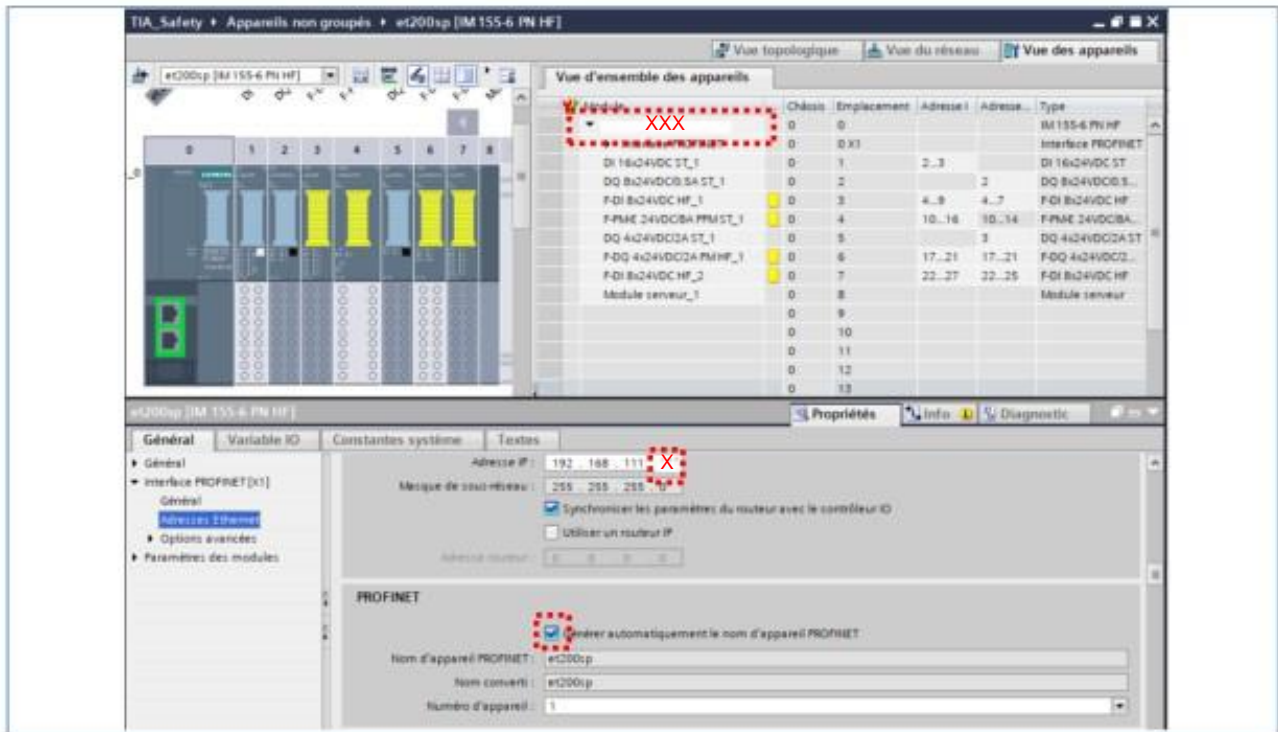
L'ET 200SP dispose de modules d'entrée et de sortie TOR. Les adresses d'E/S utilisées dans le programme STEP 7 doivent correspondre aux adresses des modules DI/DO paramétrées ici.

L'affectation d'adresses actuelle figure dans la partie inférieure de la fenêtre de travail de l'éditeur « Appareils & Réseaux », sous l'onglet « Vue des appareils » du module. Les adresses peuvent être modifiées dans le tableau.

Marche à suivre

1. Sélectionnez la « Vue des appareils » de l'ET 200SP dans l'éditeur « Appareils & Réseaux ».
2. Ouvrez le « Catalogue du matériel ».
3. Configurez la station ET 200SP en fonction de votre appareil de travail.
N'oubliez pas que les modules des emplacements 4 et 6 ouvrent un nouveau groupe de potentiel.
4. Ouvrez la « Vue d'ensemble des appareils » et reportez dans le tableau les adresses d'E/S indiquées sur la figure ci-dessus.
5. Enregistrez votre projet.

4.5.12. Exercice 12 : Affecter un nom d'appareil et une adresse IP à la station périphérique ET 200SP



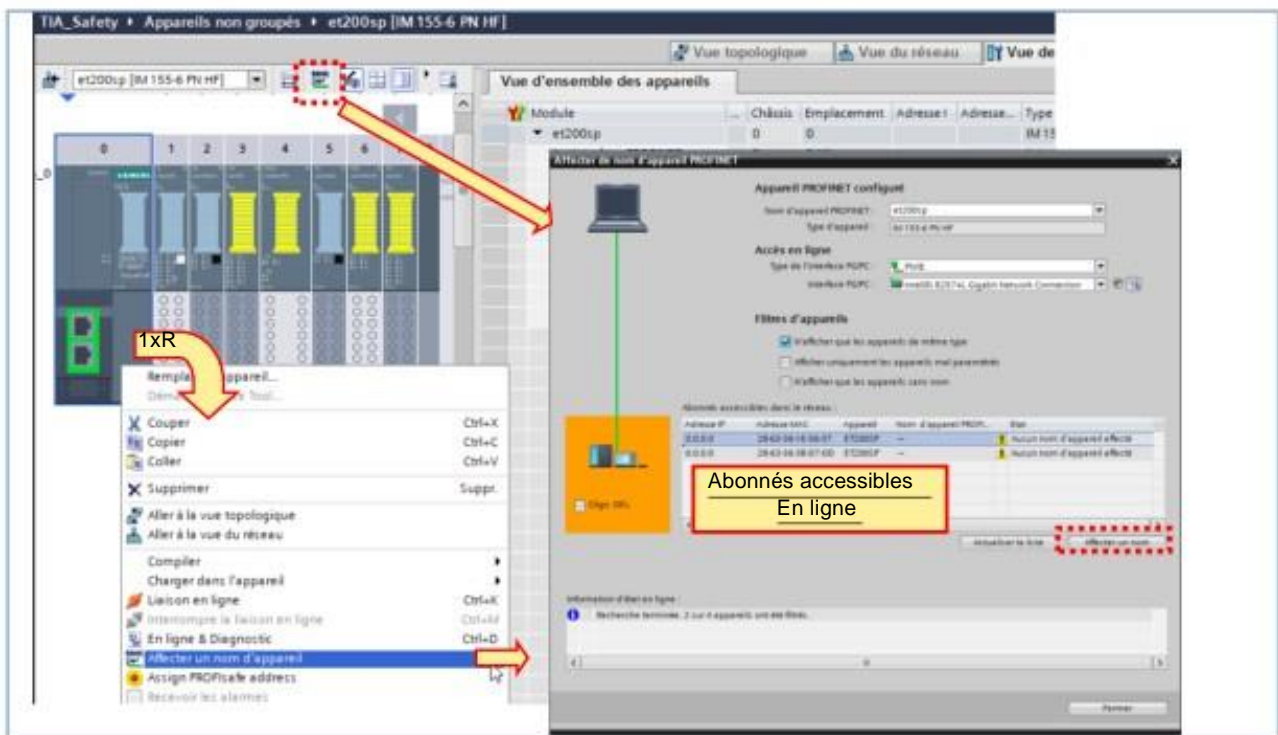
Énoncé

La station ET 200SP doit fonctionner plus tard avec l'adresse IP, le masque de sous-réseau et le nom d'appareil PROFINET figurant sur le feuillet joint à la valise.

Marche à suivre

1. Sélectionnez la « Vue des appareils » de l'ET 200SP dans l'éditeur « Appareils & Réseaux ».
2. Sélectionnez le module IM de l'emplacement 0 et ouvrez l'onglet « Propriétés » dans la fenêtre d'inspection.
3. Ouvrez la « Vue d'ensemble des appareils » et entrez le nom d'appareil correct (voir feuillet joint à la valise).
4. Sélectionnez ensuite l'onglet « Adresses Ethernet » et entrez l'adresse IP et le masque de sous-réseau sous « Protocole IP » (voir feuillet joint à la valise). Vous trouverez également sous le même onglet le « Nom d'appareil PROFINET » que vous avez précédemment édité sous l'onglet « Général ».
5. Affectez également la station ET 200SP au groupe d'appareils « Labeling machine ».
6. Enregistrez votre projet.

4.5.13. Exercice 13 : Affecter un nom d'appareil en ligne à l'ET 200SP



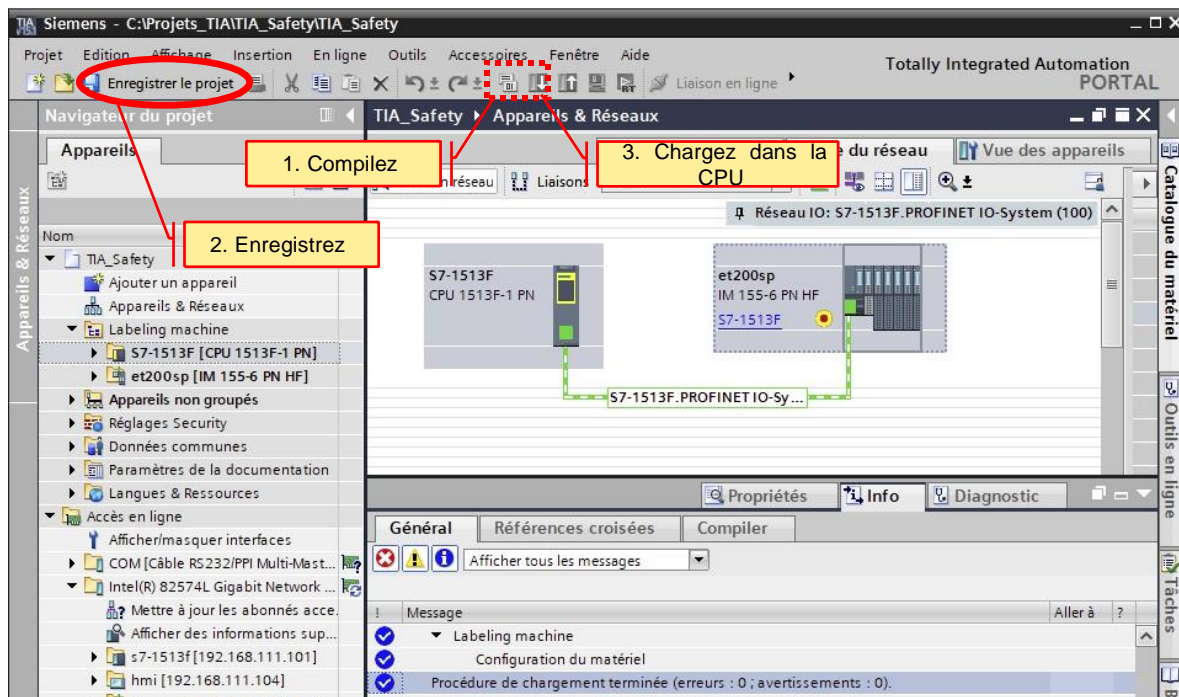
Énoncé

Le nom d'appareil PROFINET précédemment attribué hors ligne doit à présent être attribué en ligne à l'ET 200SP pour que le contrôleur d'E/S ou la CPU puisse attribuer à l'ET 200SP, lors du démarrage du système, l'adresse IP configurée hors ligne.

Marche à suivre

1. Sélectionnez la « Vue des appareils » de l'ET 200SP dans l'éditeur « Appareils & Réseaux ».
2. Cliquez avec le bouton droit de la souris sur le module d'interface ou le module de l'emplacement 0 et activez l'option « Affecter un nom d'appareil » dans le menu qui apparaît.
4. Vérifiez le nom d'appareil PROFINET (hors ligne) dans la boîte de dialogue qui apparaît.
5. Sélectionnez sous « Type d'interface PG/PC » l'interface via laquelle vous êtes connecté au PROFINET (voir figure).
6. Sélectionnez dans la partie inférieure de la boîte de dialogue, sous « Abonnés accessibles dans le réseau » (en ligne), l'ET 200SP ou le module d'interface IM156-6, puis cliquez sur « Affecter un nom ».
7. Enregistrez votre projet.

4.5.14. Exercice 14 : Compiler la configuration matérielle et la charger dans la CPU



Énoncé

Une fois le système d'E/S PROFINET entièrement configuré et paramétré, le projet doit être entièrement compilé, enregistré et chargé dans la CPU.

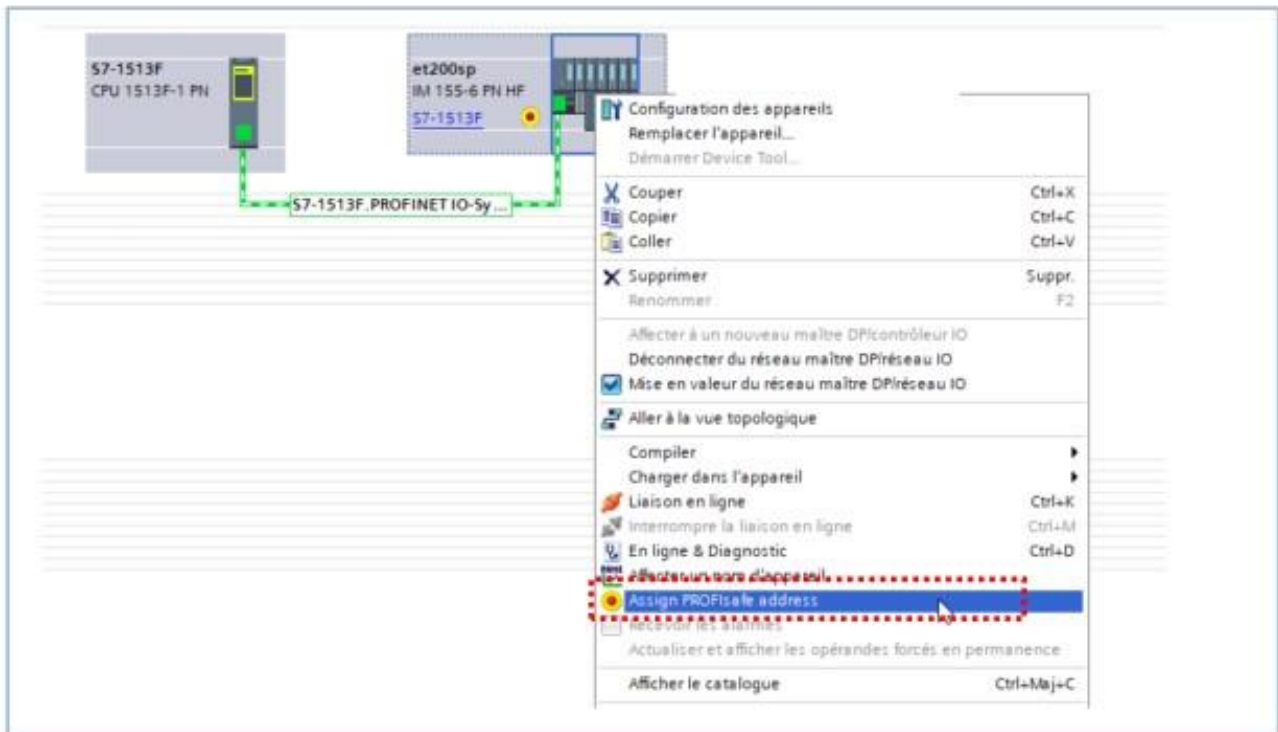
Marche à suivre

1. Compilez la configuration matérielle en sélectionnant la station S7-1500 dans le Navigateur du projet, puis en cliquant sur le bouton Compiler (voir figure). Vérifiez dans la fenêtre d'inspection, sous « Info », si la compilation a été effectuée avec succès. Si des erreurs sont apparues, corrigez-les.
2. Enregistrez votre projet.
3. Chargez la station complète dans la CPU en cliquant sur le bouton Charger (voir figure). Vérifiez dans la fenêtre d'inspection, sous « Info », si le chargement a été effectué avec succès.
4. Enregistrez votre projet.

Résultat :

L'ET 200SP devrait à présent être accessible, mais des erreurs peuvent subsister sur certains modules F.

4.5.15. Exercice 15 : ET 200SP : Attribuer les adresses F



Énoncé

Les modules de sécurité de la station ET 200SP ne possèdent pas de micro-rupteur DIP permettant d'attribuer une adresse cible F unique à chaque module. L'adresse PROFIsafe est attribuée directement à partir de STEP 7.

Les adresses de sécurité doivent à présent être attribuées en ligne à l'ET 200SP. L'attribution s'effectue via l'identification « par clignotement des LED ».

Remarque :

Il peut arriver que l'adresse cible attribuée corresponde par hasard à l'adresse cible que vous avez configurée. Si c'est le cas, l'étape 6 ne peut pas être réalisée.

Marche à suivre

1. Sélectionnez la « Vue des appareils » de l'ET 200SP dans l'éditeur « Appareils & Réseaux ».
2. Cliquez avec le bouton droit de la souris sur la station ET 200SP.
3. Dans le menu qui apparaît, activez l'option « Affecter l'adresse PROFIsafe ».
4. Dans la boîte de dialogue qui apparaît, cliquez à gauche sur la première case « Affecter ».
5. Cliquez enfin sur le bouton « Identification » pour identifier les adresses cibles.
6. Dans la boîte de dialogue, cliquez à droite sur la première case « Confirmer », puis sur le bouton « Affecter l'adresse cible F ».
7. Après attribution des adresses cibles, vous pouvez fermer la boîte de dialogue.

Résultat :

Si des erreurs devaient persister sur les modules, cela est dû au paramétrage non encore adapté des canaux des différents modules.

Le paramétrage correct sera réalisé au prochain chapitre (« Raccordement des capteurs et des actionneurs »).

Table des matières

5.	5-2	
5.	Raccordement des capteurs et des actionneurs	5-3
5.1.	Vue d'ensemble : raccordement des capteurs aux modules F-DI	5-4
5.2.	Structure des canaux DI-F (ET 200MP)	5-5
5.3.	Structure des canaux DI-F (ET 200SP)	5-6
5.4.	Paramètres DI-F	5-7
5.4.1.	Alimentation des capteurs (1)	5-7
5.4.2.	Test de court-circuit	5-8
5.4.3.	Alimentation des capteurs (2)	5-9
5.4.4.	Paramètres des canaux pour une évaluation sur 1 canal (1)	5-10
5.4.5.	Paramètres du canal pour une évaluation sur 1 canal (2)	5-11
5.4.6.	Surveillance de gigue (flottement)	5-12
5.4.7.	Paramètres des canaux pour une évaluation sur 2 canaux	5-13
5.4.8.	Comportement sur discordance	5-14
5.4.9.	Réintégration après erreur de discordance	5-16
5.4.10.	Adresses des entrées/sorties	5-17
5.4.11.	Exemples pour le raccordement d'équipements de protection électro-sensibles (ESPE) : barrières immatérielles/barrages photoélectriques/scanner laser	5-18
5.5.	Vue d'ensemble : raccordement des actionneurs au modules DQ-F	5-19
5.6.	Paramètres DQ-F	5-20
5.6.1.	Paramètres des canaux (1)	5-20
5.6.2.	Test de désactivation	5-22
5.6.3.	Allure des signaux lors du test de désactivation	5-23
5.6.4.	Test de commutation	5-24
5.6.5.	Test d'activation	5-25
5.6.6.	Allure des signaux lors du test d'activation	5-26
5.6.7.	Adresses d'E/S	5-27
5.6.8.	Exemple : raccordement d'un actionneur jusqu'à SIL3/Cat.4/PLe	5-28
5.7.	F-Power Module: F-PM-E 24VDC/8A PPM	5-30
5.8.	PM-F Paramètres des canaux	5-31
5.9.	PM-F Raccordement d'un actionneur : commutation PM / PP	5-32
5.9.1.	Commutation de charges avec liaison à la terre	5-33
5.10.	Module à relais F : F-RQ 1x24VDC/24...230VAC/5A	5-34
5.11.	Commutation du module à relais F avec DQ-F	5-35
5.12.	Énoncé : Adapter les paramètres des modules F	5-36
5.13.	Exercice 1 : Paramétrage F-DI, emplacement 3	5-37
5.13.1.	Exercice 1 (suite) : Interrupteur de maintenance, canal 0, 4	5-38
5.13.2.	Exercice 1 (suite) : Arrrt d'urgence E1, canal 1,5	5-39
5.13.3.	Exercice 1 (suite) : Arrrt d'urgence E2, canal 3, 7	5-40
5.14.	Exercice 2 : Paramétrage F-PM, emplacement 4	5-41
5.14.1.	Exercice 2 (suite) : Arrrt d'urgence E3, canal 0, 1	5-42
5.14.2.	Exercice 2 (suite) : Coupure DQ standard, canal 0	5-43
5.15.	Exercice 3 : Paramétrage F-DQ, emplacement 6	5-44
5.15.1.	Exercice 3 (suite) : Commande Moteur 1 et Moteur 2, canal 0, 1	5-45

5.16.	Exercice 4 : Paramétrage F-DI, emplacement 7.....	5-46
5.16.1.	Exercice 4 (suite) : Arrrt d'urgence E4, canal 0,4	5-47
5.16.2.	Exercice 4 (suite) : Interrupteur de sécurité RFID, canal 1,5.....	5-48
5.16.3.	Exercice 4 (suite) : Surveillance commande bimanuelle, canal 2, 6	5-49
5.17.	Exercice 5 : Compiler la configuration matérielle et la charger dans la CPU	5-50
5.18.	Information complémentaire	5-51
5.18.1.	Affectation des bornes ET200SP / F-DI.....	5-52
5.18.2.	Affectation des bornes ET200SP / F-DQ	5-53
5.18.3.	Affectation des bornes ET200SP / F-PM.....	5-54
5.18.4.	Affectation des bornes ET200SP / F-RQ	5-55
5.19.	Catégories d'arrrt selon EN 60204-1.....	5-56
5.20.	SINAMICS G120 : STO / SS1 en PL(e) SIL3 Arrrt d'urgence via bornes sur le PM240-2 FSD-FSF	5-57
5.21.	Aides à la mise en œuvre de la technique de sécurité	5-58

5.

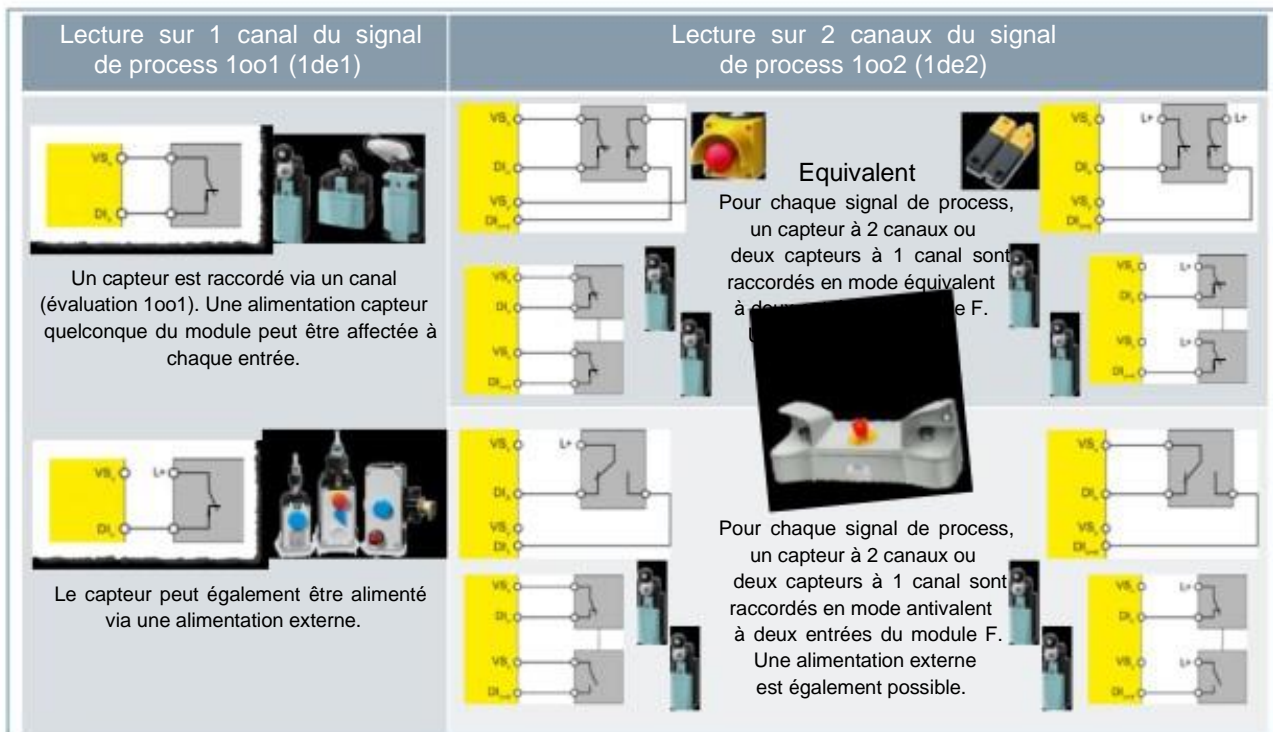
5. Raccordement des capteurs et des actionneurs

À l'issue de la formation, le participant au stage

- ... sera capable d'expliquer comment un capteur doit être raccordé et le module paramétré
- ... sera capable d'expliquer comment un actionneur doit être raccordé et le module paramétré
- ... connaîtra les différentes mesures de détection des erreurs d'un module de sécurité
- ... saura paramétrer les modules d'entrée et sortie de sécurité de l'automate de formation en fonction du câblage des appareils de formation



5.1. Vue d'ensemble : raccordement des capteurs aux modules F-DI



Évaluation 1oo1 (1de1)

Lors de l'évaluation 1oo1 (1de1), le capteur n'est présent qu'une seule fois.

Alimentation du capteur

L'alimentation du capteur peut s'effectuer de manière interne ou externe.

Raccordement du capteur via 1 canal

Un capteur est raccordé via 1 canal pour chaque signal de process (évaluation 1oo1 ; 1de1). À chaque entrée peut être affectée une alimentation capteur quelconque du module. Si le test de court-circuit n'est pas activé ou si l'alimentation des capteurs est réglée sur « Alimentation externe des capteurs » pour les entrées TOR, vous devez poser le câble de manière à prévenir tout risque de court-circuit.

Évaluation 1oo2 (1de2), équivalent/antivalent

Lors de l'évaluation 1oo2 (1de2) équivalent/antivalent, deux canaux d'entrée sont utilisés par :

- un capteur à 2 canaux
- deux capteurs à 1 canal
- un capteur antivalent

Une vérification interne d'égalité (équivalence) ou d'inégalité (antivalence) est effectuée sur les signaux d'entrée.

Notez que deux canaux sont réunis en une paire de canaux lors de l'évaluation 1oo2 (1de2). Le nombre de signaux de process disponibles du module F se réduit en conséquence.

Schéma de câblage

Pour chaque signal de process, un capteur à 2 canaux équivalent ou deux capteurs à 1 canal détectant la même valeur de process sont raccordés à deux entrées du module F.

5.2. Structure des canaux DI-F (ET 200MP)

Numéros des canaux et MIE pour DI-F (Adresse 10)

0	I 10.0	8	I 11.0
1	I 10.1	9	I 11.1
2	I 10.2	10	I 11.2
3	I 10.3	11	I 11.3
4	I 10.4	12	I 11.4
5	I 10.5	13	I 11.5
6	I 10.6	14	I 11.6
7	I 10.7	15	I 11.7

Important:
Pour la lecture des 2 canaux d'un signal du processus via le module (équivalent, antivalent) l'utilisateur ne dispose que du bit de poids faible pour son programme (I 10.0 pour canal 0)

Paire de canaux

General
Module parameters
Inputs 0 - 15
General
F-parameters
Inputs
Sensor supply
Channel parameters
Channel 0, 8
Channel 0
Channel 8
Channel 1, 9
Channel 1
Channel 9
Channel 2, 10
Channel 3, 11
Channel 4, 12
Channel 5, 13
Channel 6, 14
Channel 7, 15
I/O addresses

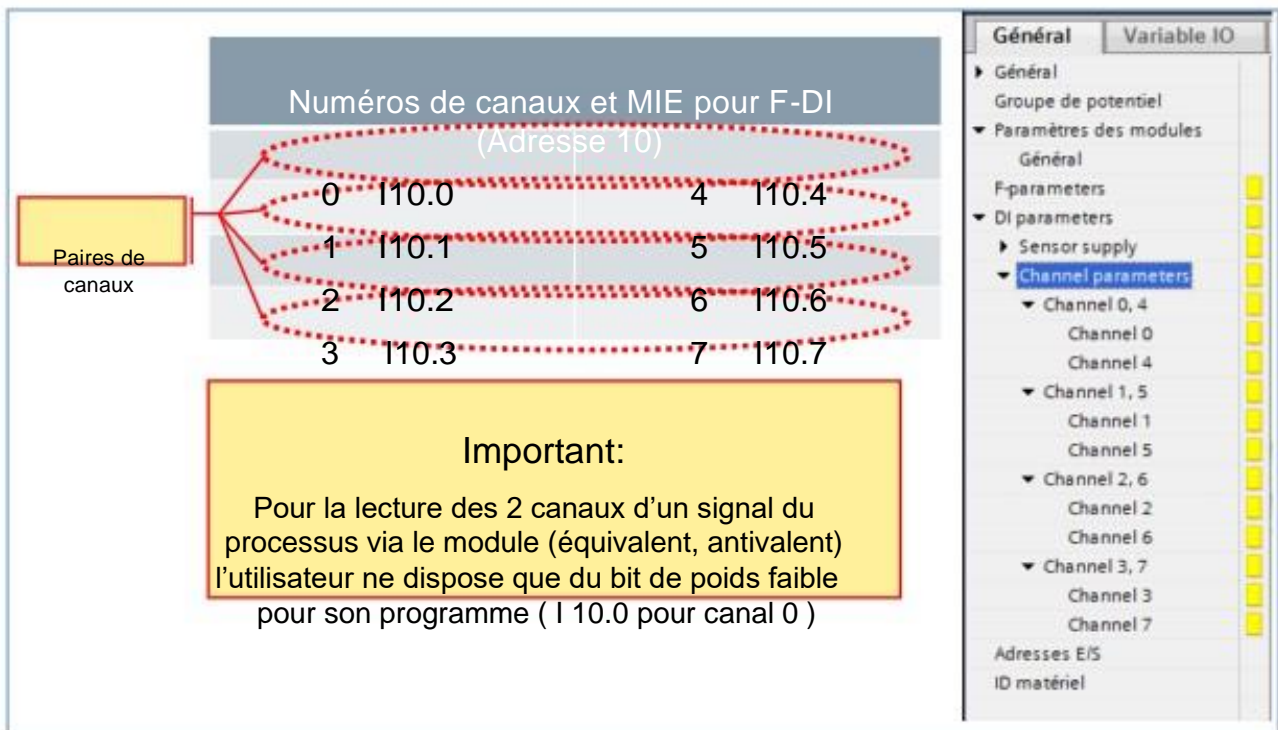
Païres et adresses des canaux

Avec des capteurs à 1 canal et une évaluation 1oo1, l'appartenance d'un canal à une paire de canaux n'a pas d'importance. Chaque canal de la paire de canaux est évalué indépendamment de l'autre et possède sa propre adresse individuelle

Avec une évaluation 1oo2, les signaux des capteurs doivent être câblés avec les canaux du module qui peuvent être évalués par le module comme paire de canaux ou sur lesquels une analyse de discordance peut être effectuée (sur la diapositive ci-dessus : paires de canaux (0,8) ainsi que (1,9) et (2,10)).

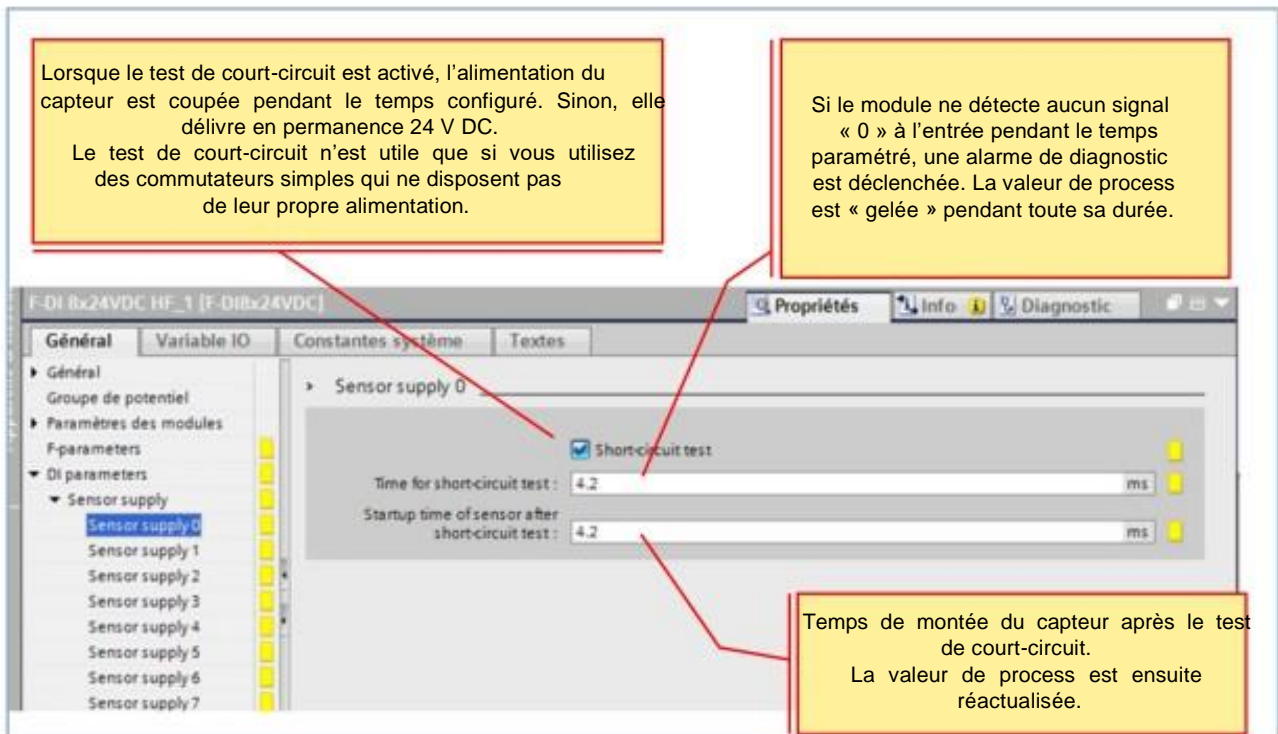
Avec une évaluation 1oo2, une paire de canaux occupe toujours la plus petite adresse d'entrée et c'est la seule disponible dans le programme.

5.3. Structure des canaux DI-F (ET 200SP)



5.4. Paramètres DI-F

5.4.1. Alimentation des capteurs (1)



Test de court-circuit

Ce paramètre permet d'activer la détection de court-circuit pour les canaux du module F pour lesquels une alimentation interne des capteurs est retenue. Le test de court-circuit n'est utile que si vous utilisez des commutateurs simples qui ne disposent pas de leur propre alimentation. Le test de court-circuit n'est pas possible pour les commutateurs avec alimentation comme les détecteurs de proximité 3/4 fils.

La détection de court-circuit désactive brièvement l'alimentation capteur. La durée de désactivation est égale au « temps de test de court-circuit » configuré. Lorsqu'un court-circuit est détecté, le module F déclenche une alarme de diagnostic et l'entrée est passivée.

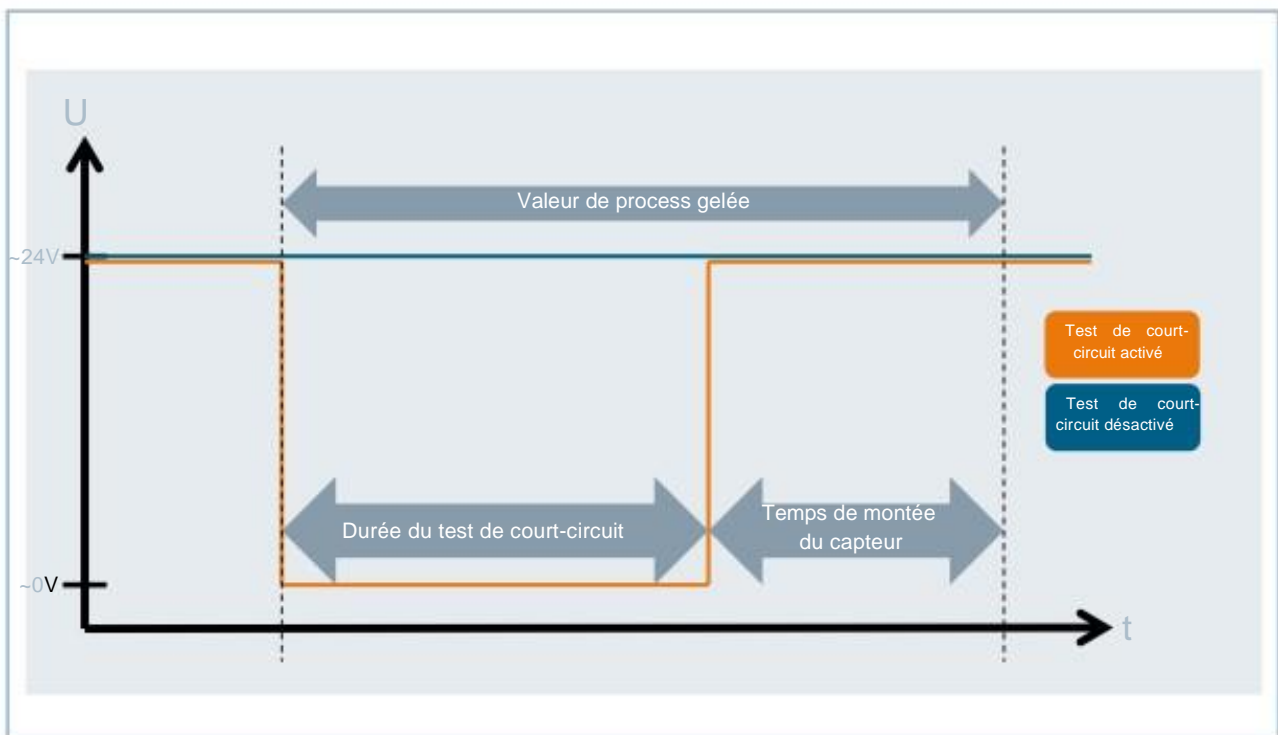
Les courts-circuits suivants sont détectés :

- Court-circuit entre l'entrée et L+
- Court-circuit entre l'entrée et un autre canal lorsque celui-ci affiche un signal 1
- Court-circuit entre l'entrée et l'alimentation capteur d'un autre canal
- Court-circuit entre l'alimentation capteur et l'alimentation capteur d'un autre canal

Lorsque le test de court-circuit est désactivé, vous devez veiller à poser vos câbles de manière à prévenir tout risque de court-circuit et de court-circuit transversal ou choisir un type de raccordement (discordance, antivalent) capable de détecter également les courts-circuits transversaux via la discordance.

Pendant la durée d'exécution du test de court-circuit (temps du test de court-circuit + temps de montée du capteur après le test de court-circuit), la dernière valeur valide de l'entrée avant le démarrage du test de court-circuit est transmise à la F-CPU. L'activation du test de court-circuit a donc une incidence sur le temps de réaction des différents canaux ou paires de canaux.

5.4.2. Test de court-circuit



Temps du test de court-circuit

Lorsque le test de court-circuit est activé, l'alimentation du capteur concerné est coupée pendant le temps paramétré. Si le module ne détecte aucun signal « 0 » à l'entrée pendant le temps paramétré, un message de diagnostic est généré.

Lors du paramétrage, tenez compte des éléments suivants :

- Si le canal est passivé, cela peut être dû à une capacité trop élevée entre l'alimentation capteur et l'entrée. Celle-ci est composée de la capacité linéique du câble et de la capacité du capteur utilisé. Si la capacité connectée ne se décharge pas pendant le temps paramétré, vous devez ajuster le paramètre « Temps de test de court-circuit ».
- Les valeurs de temps disponibles pour le retard à l'entrée dépendent du « temps de montée du capteur après le test de court-circuit » et du « temps de test de court-circuit » de l'alimentation capteur paramétrée.

Temps de montée du capteur après le test de court-circuit

Pour réaliser le test de court-circuit, il convient d'indiquer un temps de montée en plus du temps de coupure (« Temps de test de court-circuit »). Ce paramètre vous permet d'indiquer au module le temps de montée nécessaire au capteur utilisé après l'établissement de l'alimentation capteur. Vous évitez ainsi d'avoir un état d'entrée indéfini du fait des transitoires du capteur.

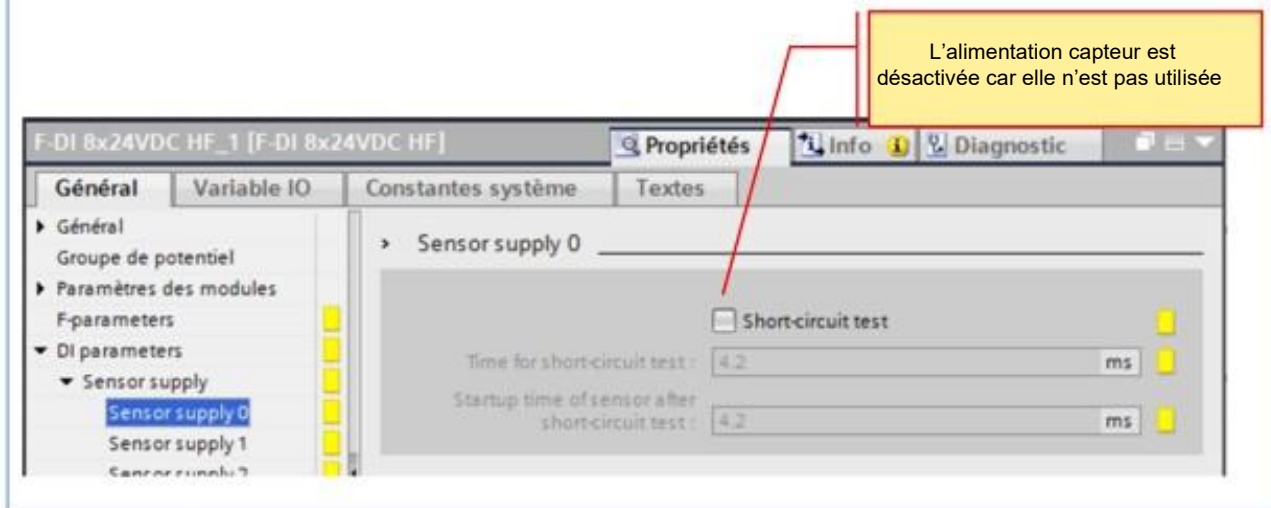
Lors du paramétrage, tenez compte des éléments suivants :

- Ce paramètre doit être supérieur au temps d'établissement du capteur utilisé.
- Comme le temps paramétré a une incidence sur le temps de réaction du module, nous vous recommandons de régler ce temps à une valeur aussi faible que possible, mais suffisamment élevée pour que votre capteur ait atteint un état stable.
- Les valeurs de temps disponibles pour le retard à l'entrée dépendent du « temps de montée du capteur après le test de court-circuit » et du « temps de test de court-circuit » de l'alimentation capteur paramétrée.

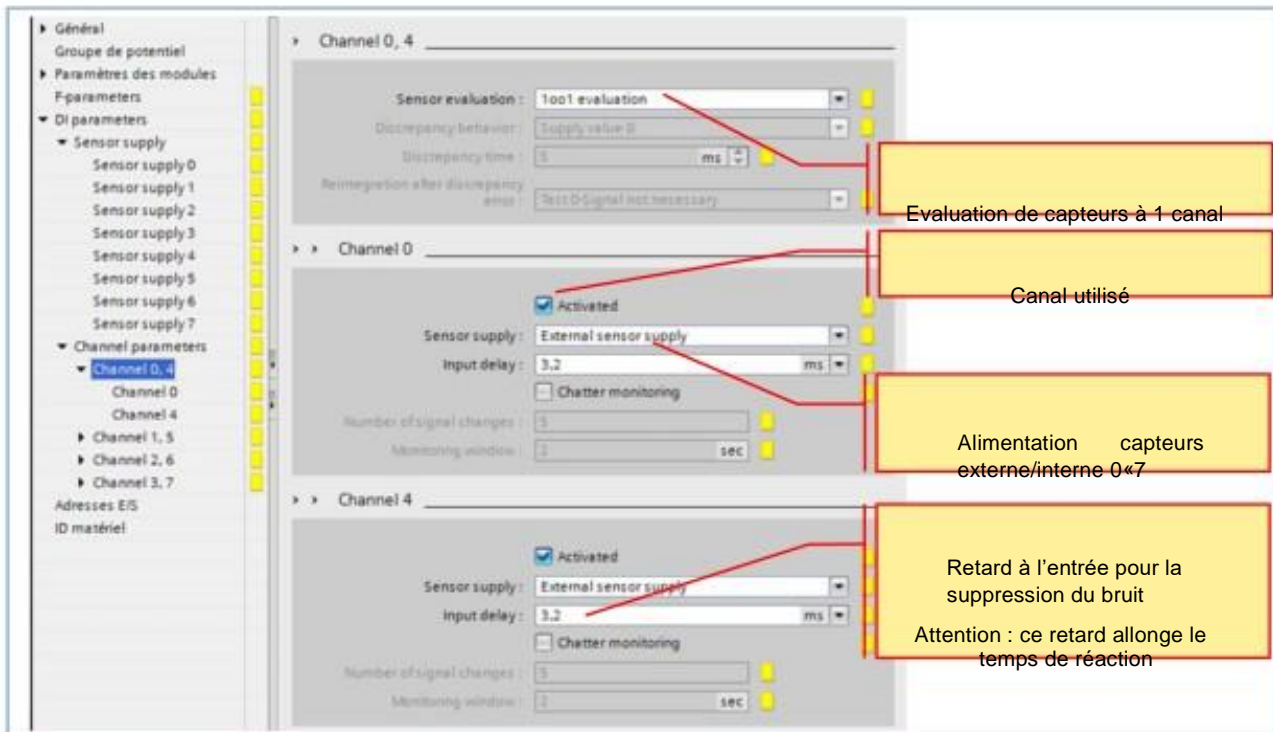
5.4.3. Alimentation des capteurs (2)

Alimentations des capteurs

- Chaque alimentation peut être utilisée pour chaque entrée
- Si vous n'utilisez pas une alimentation, elle est désactivée



5.4.4. Paramètres des canaux pour une évaluation sur 1 canal (1)



Activé

Pour réduire les sollicitations de la CPU ou accélérer l'actualisation de la mémoire image des entrées (MIE), il est conseillé de désactiver les entrées non utilisées.

Évaluation des capteurs et connexion

Évaluation 1de1 (1oo1)

Lors de l'évaluation 1de1, le capteur est présent une seule fois et est raccordé au module F-DI via 1 canal.

Si la qualité du capteur est inférieure à celle requise par la classe de sécurité nécessaire, le capteur doit être mis en œuvre de manière redondante et raccordé sur 2 canaux.

Alimentation des capteurs

Choisissez ici soit l'une des alimentations internes des capteurs VS_0 à VS_n , soit une alimentation externe des capteurs. Le choix d'une alimentation interne est la condition préalable à l'utilisation du test de court-circuit.

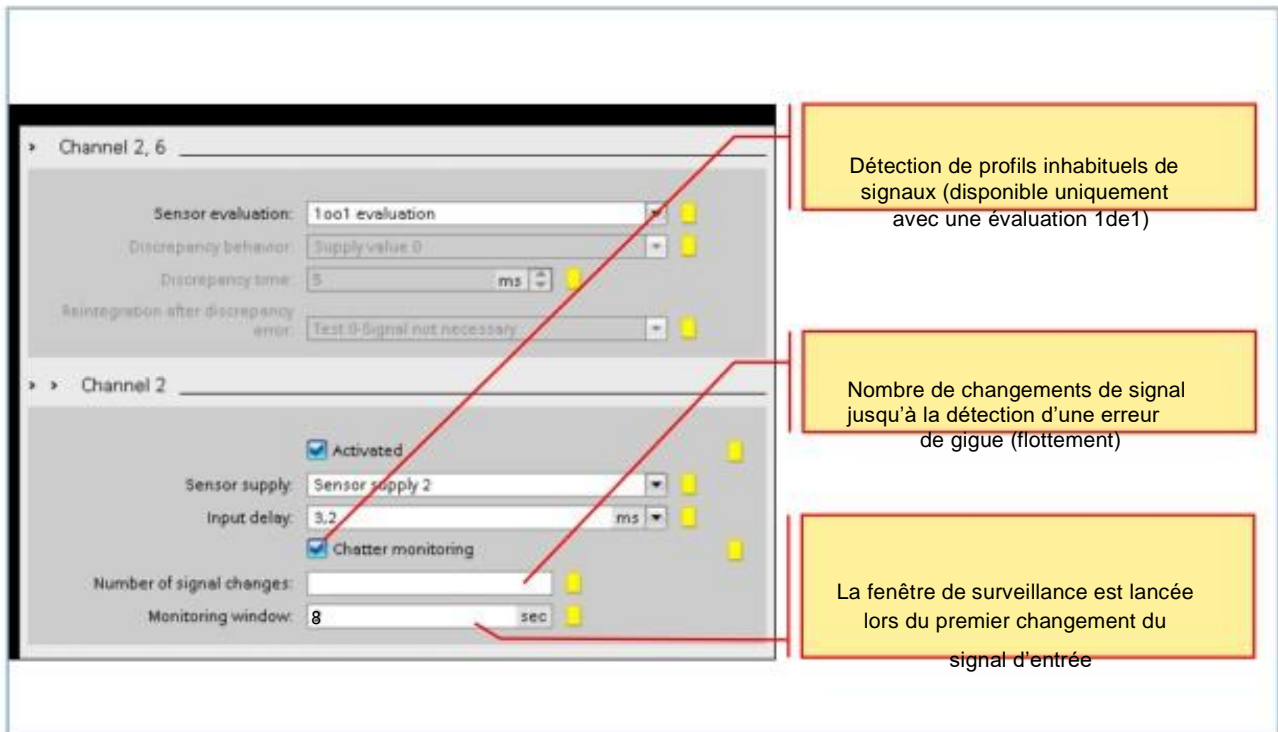
Retard à l'entrée

C'est le temps minimal pendant lequel un signal d'entrée modifié doit être présent sur le module pour qu'un nouveau signal soit détecté et codé. Le retard à l'entrée sert à supprimer les brèves impulsions parasites (« anti-rebond »).

Pour supprimer les perturbations couplées, vous pouvez paramétrer un retard à l'entrée pour un canal ou une paire de canaux.

Les impulsions parasites dont le temps d'impulsion est inférieur au retard à l'entrée paramétré (en ms) sont supprimées. Les impulsions parasites supprimées ne sont pas visibles dans la MIE. Un retard à l'entrée élevé supprime les impulsions parasites plus longues, mais entraîne un temps de réaction plus long. Les valeurs de temps disponibles pour le retard à l'entrée dépendent du « temps de montée du capteur après le test de court-circuit » et du « temps de test de court-circuit » de l'alimentation capteur paramétrée.

5.4.5. Paramètres du canal pour une évaluation sur 1 canal (2)



Surveillance de gigue (flottement)

La surveillance de gigue est une fonction de supervision des signaux d'entrée TOR. Elle détecte et signale, avec une évaluation 1oo1 (1de1), les allures de signaux anormales du point de vue du processus, comme une fluctuation trop fréquente du signal d'entrée entre « 0 » et « 1 ». L'apparition de telles anomalies de signaux est le signe de capteurs défectueux ou de l'existence d'instabilités dans le processus. Une fenêtre de surveillance paramétrée est disponible pour chaque canal d'entrée. La fenêtre de surveillance est lancée par le premier changement du signal d'entrée. Si, dans la fenrtre de surveillance, le signal d'entrée change au moins aussi souvent que le « nombre de changements de signal » paramétré, une erreur de gigue est détectée. Si aucune erreur de gigue n'est détectée dans la fenrtre de surveillance, la fenêtre est relancée au prochain changement de signal. Si une erreur de gigue est détectée, un diagnostic s'affiche. Si aucune erreur de gigue n'apparaît sur trois fois la durée paramétrée pour la fenrtre de surveillance, le diagnostic est réinitialisé.

Nombre de changements de signal

Définit le nombre de changements de signal au-delà duquel une erreur de gigue doit être signalée.

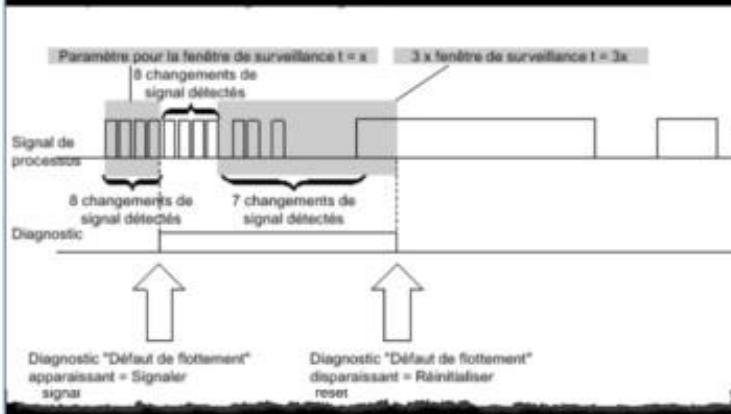
Fenêtre de surveillance

Définit le temps de la fenêtre de surveillance de gigue. Vous pouvez régler des durées comprises entre 1 et 100 s en secondes entières. Si vous réglez sur 0 s, vous pouvez paramétrer une fenêtre de surveillance de 0,5 s.

5.4.6. Surveillance de gigue (flottement)

Surveillance du flottement

Pour chaque canal d'entrée, une fenêtrre de surveillance dédiée est disponible. La fenêtrre de surveillance commence par le premier changement de signal du signal d'entrée. Si le signal d'entrée de la fenêtrre de surveillance change de manière au moins aussi fréquente que le « Nombre de changements de signal », un défaut de flottement est détecté. Si aucun défaut de flottement n'est détecté dans la fenêtrre de surveillance, le changement de signal suivant lancera de nouveau la fenêtrre de surveillance.



Diagnostic de défaut de flottement

Lorsqu'un défaut de flottement est détecté, un diagnostic est transmis. Si le défaut de flottement ne survient plus pendant une période de trois fois le temps configuré, le diagnostic sera retiré.

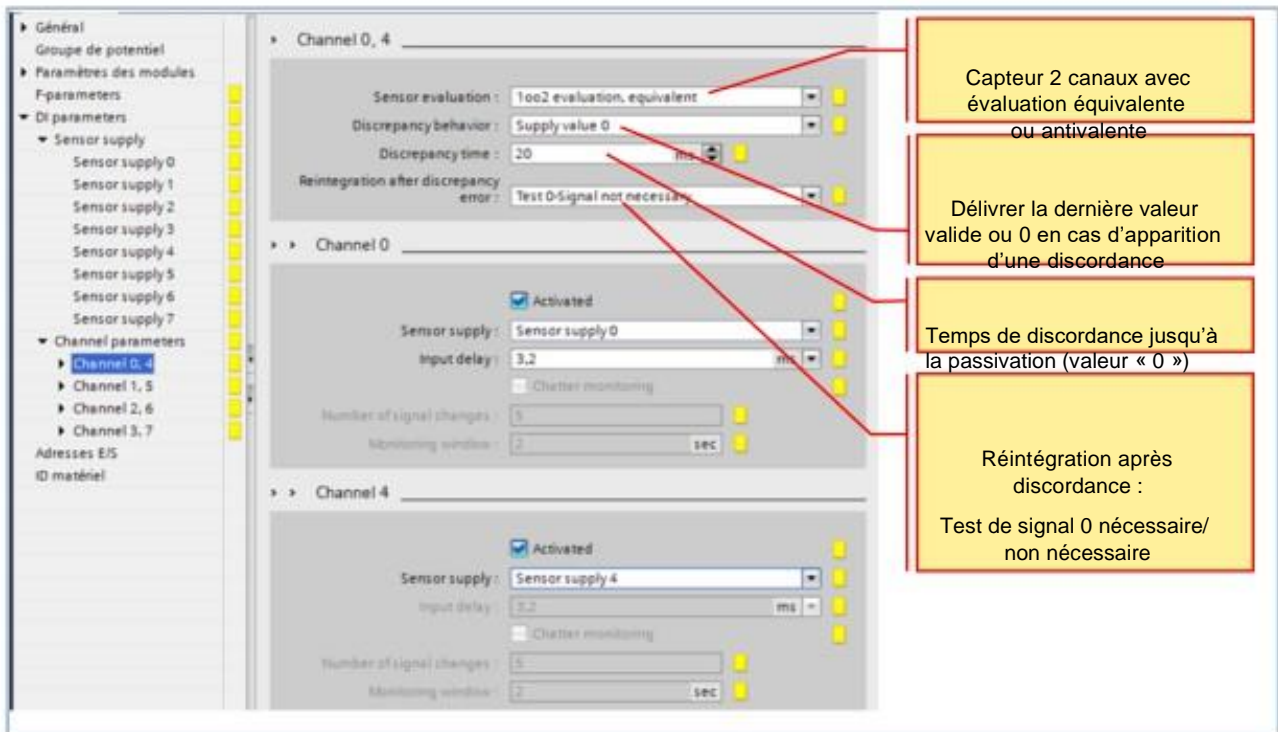
Surveillance de gigue

Une fenêtrre de surveillance spécifique est disponible pour chaque canal d'entrée. La fenêtrre de surveillance est lancée au premier changement du signal d'entrée. Si le signal d'entrée de la fenêtrre de surveillance change au moins aussi souvent que le « nombre de changements de signal » paramétré, une erreur de gigue est détectée. Si aucune erreur de gigue n'est détectée dans la fenêtrre de surveillance, la fenêtrre est relancée au prochain changement de signal.

Diagnostic de gigue

Un diagnostic s'affiche dès qu'une erreur de gigue est détectée. Si aucune erreur de gigue n'apparaît dans un intervalle égal à trois fois le temps paramétré, le diagnostic est réinitialisé.

5.4.7. Paramètres des canaux pour une évaluation sur 2 canaux



Évaluation 1oo2 (1de2), équivalent/antivalent

Lors de l'évaluation 1oo2 (1de2) équivalent/antivalent, deux canaux d'entrée sont utilisés par :

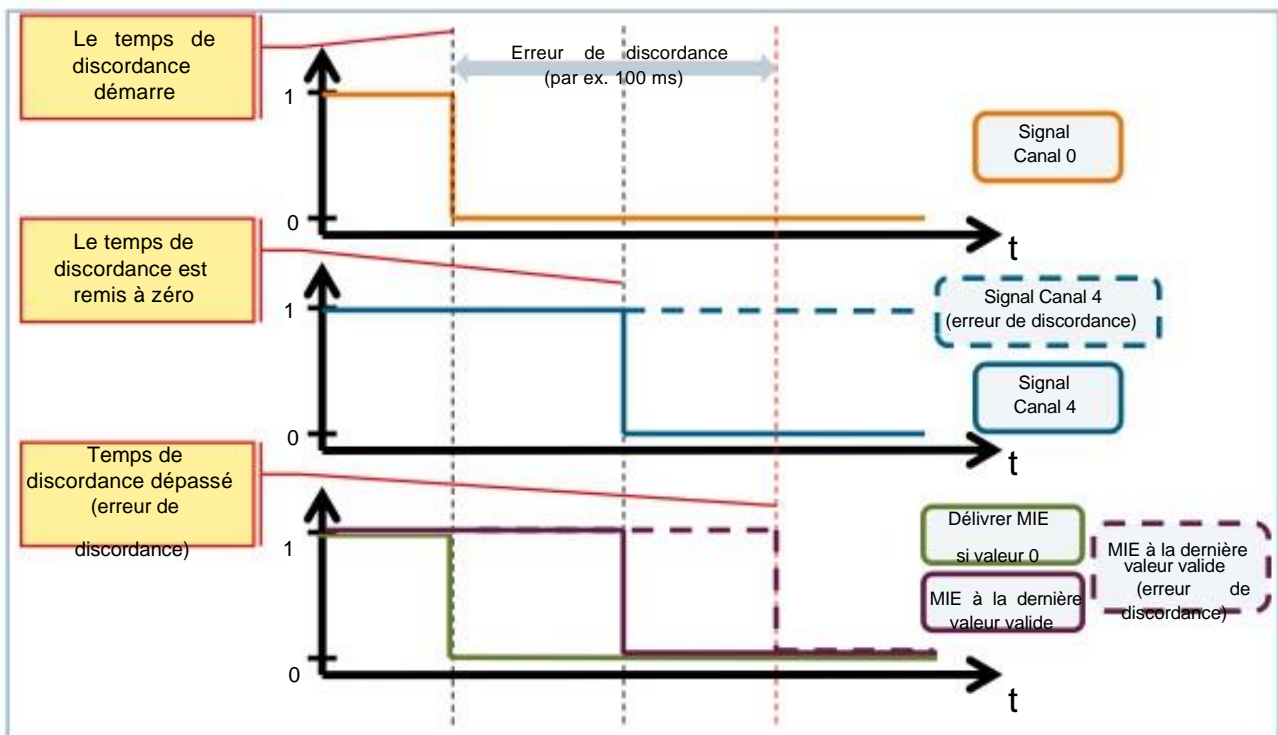
- un capteur à 2 canaux
- deux capteurs à 1 canal
- un capteur antivalent

Une vérification interne d'égalité (équivalence) ou d'inégalité (antivalence) est effectuée sur les signaux d'entrée. Notez que deux canaux sont réunis en une paire de canaux lors de l'évaluation 1oo2 (1de2). Le nombre de signaux de process disponibles du module F se réduit en conséquence.

Analyse de discordance

Si vous utilisez un capteur à 2 canaux ou deux capteurs à 1 canal qui acquièrent la même valeur de process physique, les capteurs peuvent réagir avec un retard du fait, par exemple, de la précision limitée de leur agencement. L'analyse de discordance sur équivalence/antivalence s'utilise pour les entrées de sécurité afin de détecter les incohérences temporelles entre deux signaux ayant la même fonction. L'analyse de discordance démarre lorsque des niveaux différents (ou des niveaux identiques en cas de contrôle d'antivalence) de deux signaux associés sont détectés. Le système vérifie si, après écoulement d'un temps paramétrable, la différence (ou l'égalité en cas de contrôle d'antivalence) a disparu. Si ce n'est pas le cas, il y a erreur de discordance.

5.4.8. Comportement sur discordance



Comportement sur discordance

Le « Comportement sur discordance » vous permet de paramétrer la valeur mise à la disposition du programme de sécurité de la F-CPU pendant la discordance entre les deux canaux d'entrée concernés, c'est-à-dire durant l'écoulement du temps de discordance. Le comportement sur discordance peut être paramétré comme suit :

- « Délivrer la dernière valeur valide »
- « Délivrer la valeur 0 »

Pour définir le comportement du canal du module durant l'écoulement du temps de discordance, 2 paramétrages sont possibles :

« Délivrer la dernière valeur valide »

La dernière valeur valide avant l'apparition de la discordance (ancienne valeur) est mise à la disposition du programme de sécurité de la F-CPU dès qu'une discordance entre les signaux des deux canaux d'entrée est détectée. Cette valeur est disponible jusqu'à ce que la discordance ait disparu ou jusqu'à ce que le temps de discordance se soit écoulé et qu'une erreur de discordance soit détectée. Après écoulement du temps de discordance, la valeur « 0 » est transmise dans tous les cas au programme de sécurité de la CPU en cas de détection d'une erreur de discordance.

Attention :

Le fait qu'une erreur de discordance ne soit détectée qu'après écoulement du temps de discordance allonge le temps de réaction de l'automate. Si des réactions très rapides de l'automate sont exigées pour des raisons de sécurité en cas d'erreur, le temps de discordance ne doit pas être réglé à des valeurs plus grandes que nécessaires.

« Délivrer la valeur 0 »

Avec ce paramétrage, le temps de réaction de l'automate n'est pas allongé, car la valeur de sécurité « 0 » est directement transmise au programme de sécurité de la F-CPU durant l'écoulement du temps de discordance. La valeur « 0 » correspond à la valeur qui serait de toute façon transmise à la CPU en cas d'erreur (c'est-à-dire après l'écoulement du temps de discordance).

Temps de discordance

Le comportement sur discordance n'a d'intérêt que durant l'écoulement du temps de discordance. Si la discordance persiste après l'écoulement du temps de discordance, le module détecte cet état comme une erreur et transmet (comme toujours en cas d'erreur) la valeur « 0 » pour le canal concerné à la F-CPU.

Dans la plupart des cas, le temps de discordance est lancé, mais ne s'écoule pas entièrement, car les différences entre les signaux sont rapidement compensées.

Choisissez un temps de discordance suffisamment grand pour qu'en l'absence d'erreur, la différence entre les deux signaux (ou la concordance en cas de contrôle d'antivalence) ait disparu avant l'écoulement du temps de discordance.

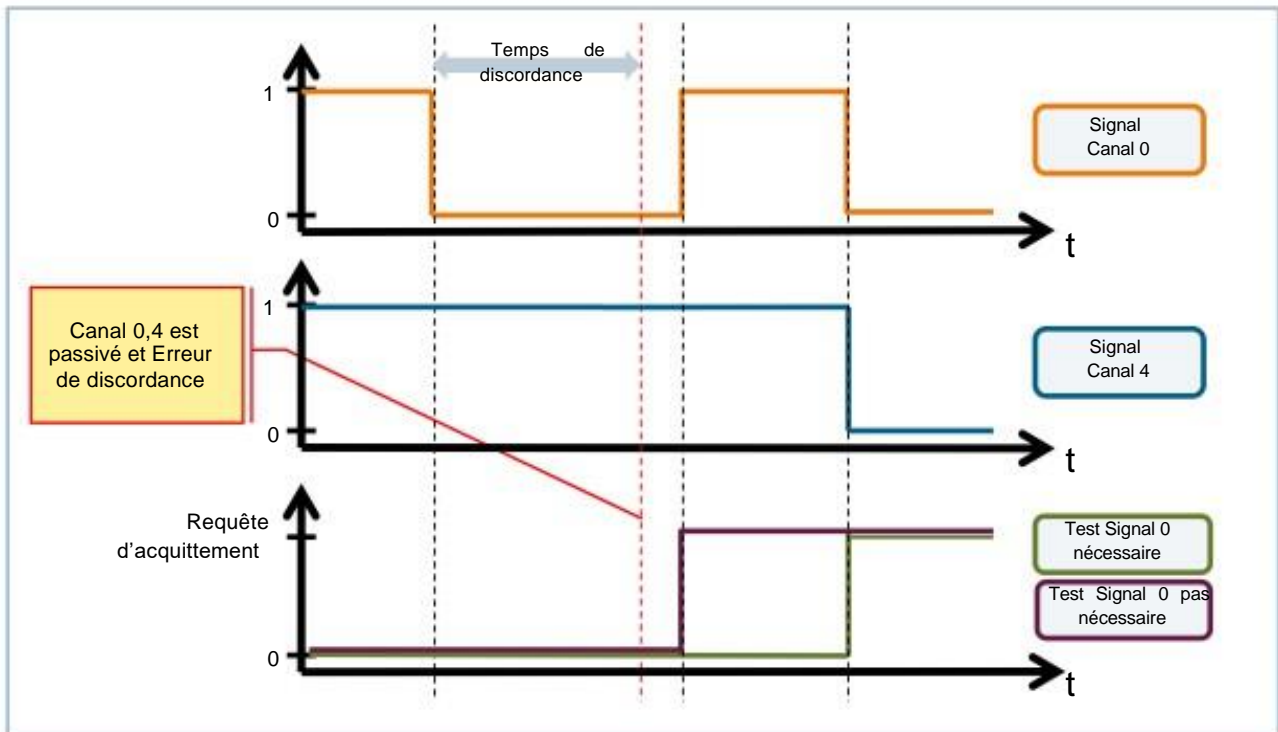
Comportement pendant l'écoulement du temps de discordance

Pendant l'écoulement interne du temps de discordance paramétré, les canaux d'entrée concernés mettent à la disposition du programme de sécurité de la F-CPU soit la dernière valeur valide, soit la valeur « 0 » selon le paramétrage du comportement sur discordance.

Comportement après l'écoulement du temps de discordance

Si, après écoulement du temps de discordance paramétré, aucune concordance (ou discordance en cas de contrôle d'antivalence) des signaux d'entrée n'est présente (par ex. en cas de rupture de fil sur un câble de capteur), une erreur de discordance est détectée et le message de diagnostic « Erreur de discordance » est généré avec indication des canaux défectueux.

5.4.9. Réintégration après erreur de discordance



Réintégration après une erreur de discordance

Ce paramètre vous permet de définir quand une erreur de discordance est considérée comme corrigée et donc une réintégration des canaux d'entrée concernés comme possible. Vous disposez des possibilités de paramétrage suivantes :

- « Test de signal 0 nécessaire »
- « Test de signal 0 non nécessaire »

Conditions préalables

Vous avez effectué le paramétrage suivant :

- « Évaluation des capteurs » : « Évaluation 1oo2 (1de2), équivalent » ou « Évaluation 1oo2 (1de2), antivalent »

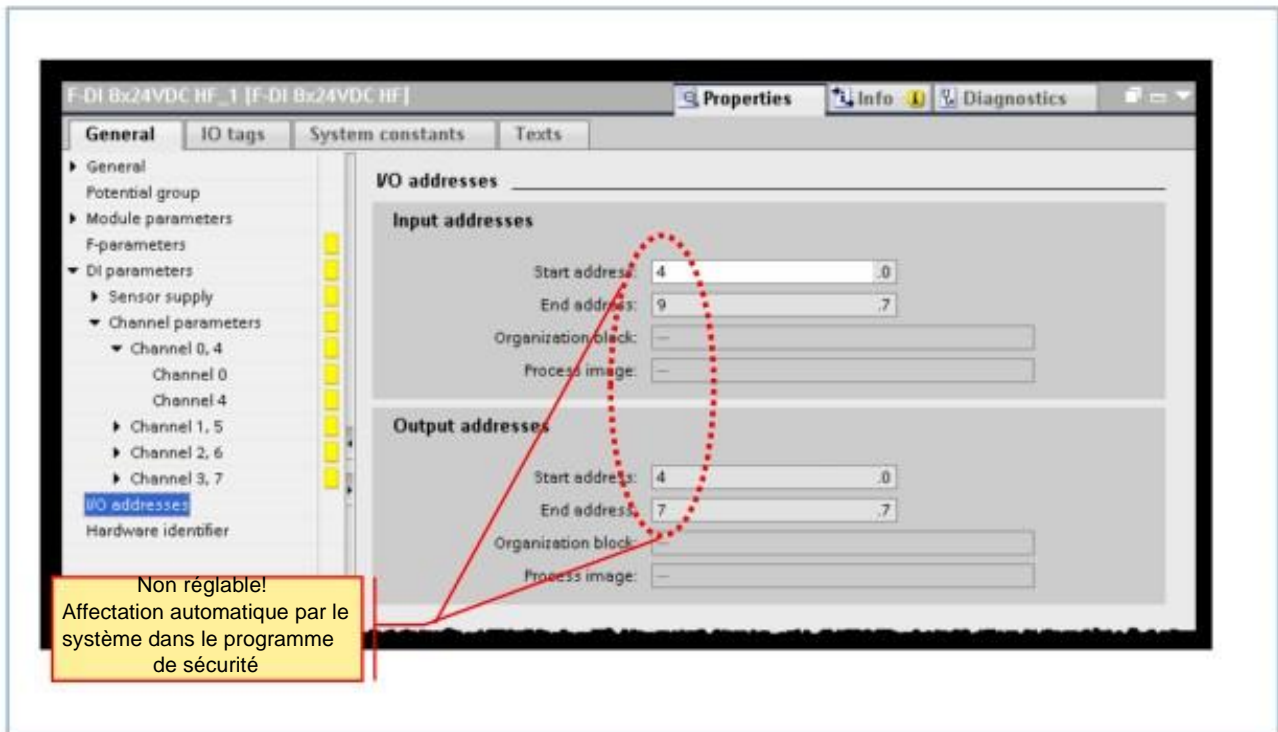
« Test de signal 0 nécessaire »

Si vous avez paramétré « Test de signal 0 nécessaire », une erreur de discordance est considérée comme corrigée si le signal 0 est à nouveau présent aux deux canaux d'entrée concernés. Si vous utilisez des capteurs antivalents, c'est-à-dire si vous avez réglé « Évaluation des capteurs » sur « Évaluation 1oo2 (1de2), antivalent », le signal 0 doit être à nouveau présent sur le canal de plus faible poids de la paire de canaux.

« Test de signal 0 non nécessaire »

Si vous avez paramétré « Test de signal 0 non nécessaire », une erreur de discordance est considérée comme corrigée s'il n'y a plus de discordance aux deux canaux d'entrée concernés.

5.4.10. Adresses des entrées/sorties



Adresses des entrées et sorties

Les adresses des modules d'entrée et sortie de sécurité sont librement paramétrables comme avec les modules standard. Pour le traitement de la communication de sécurité PROFIsafe, les modules d'entrée ou de sortie de sécurité utilisent, outre les données utiles d'entrée ou de sortie, des octets supplémentaires dans la mémoire image des entrées et des sorties. Un module F-DI occupe donc également des octets dans la mémoire image des sorties, un module F-DQ également des octets dans la mémoire image des entrées.

Vous ne pouvez accéder qu'aux adresses occupées par des données utiles et des états de valeur. Les autres zones d'adresses occupées par les modules F sont entre autres réservées à la communication de sécurité entre les modules F et la F-CPU en conformité avec PROFIsafe.

En cas d'évaluation 1oo2 (1de2) des capteurs, les deux canaux sont regroupés.

En cas d'évaluation 1oo2 (1de2) des capteurs, vous ne pouvez accéder dans le programme de sécurité qu'au canal de poids faible.

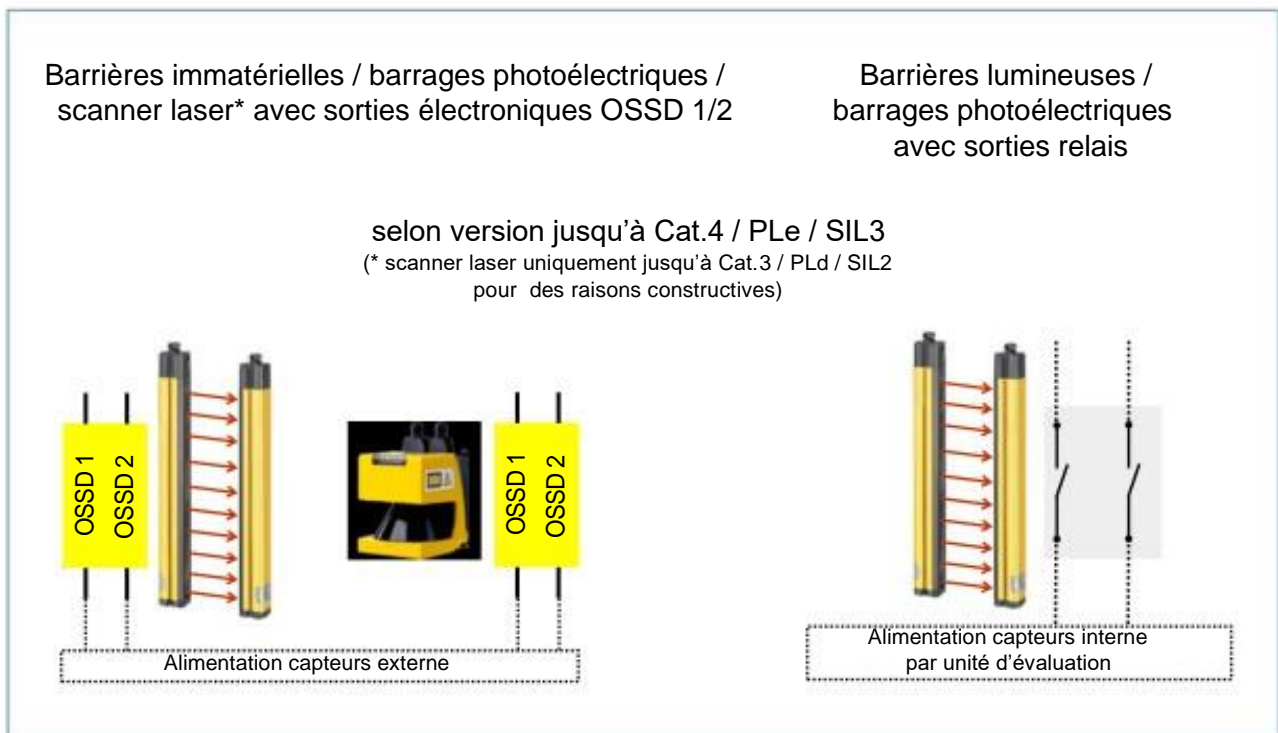
Mémoire image

Outre les mémoires image MIE et MIS automatiquement actualisées par le système d'exploitation, la CPU peut offrir jusqu'à 15 mémoires image partielles (MIP) paramétrables (MIP 1 à MIP 15 max. selon la CPU). Il est donc possible d'actualiser, indépendamment de la mémoire image OB1 actualisée de manière cyclique (MI OB1), des mémoires image partielles (MIP) en fonction du traitement des OB d'alarme. Chaque zone d'adresses d'E/S ou chaque module d'entrée ou de sortie ne peut être affecté qu'à une mémoire image partielle. Si un module est affecté à l'une des mémoires image partielles (MIP), il ne peut plus faire partie de la mémoire image cyclique (MI OB1).

IMPORTANT :

Si vous utilisez les I/O en mode sécurité, la sélection n'est pas possible. La mémoire image est actualisée automatiquement au début et à la fin de l'OB-F

5.4.11. Exemples pour le raccordement d'équipements de protection électro-sensibles (ESPE) : barrières immatérielles/barrages photoélectriques/scanner laser



ESPE (équipements de protection électro-sensibles)

- ... à sorties électroniques

Les capteurs à sorties OSSD (Output Signal Switching Device = dispositif de commutation du signal de sortie) disposent d'une détection de court-circuit/court-circuit transversal intégrée. Celle-ci doit donc être désactivée côté unité d'évaluation (dans HW Config pour les modules F-DI).

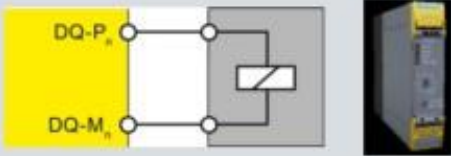
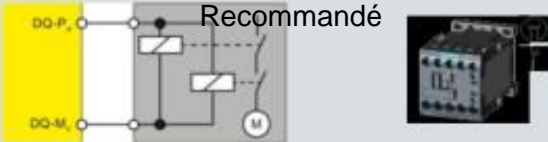
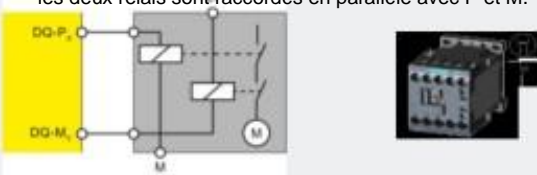
- ... à sorties relais

Les capteurs à sorties relais ne peuvent pas réaliser de détection de court-circuit/court-circuit transversal via leurs contacts libres de potentiel.

Dans les applications en Cat.4 / PLe / SIL3, la détection de court-circuit/court-circuit transversal doit donc être activée côté unité d'évaluation (dans Configuration d'appareils pour les modules F-DI).

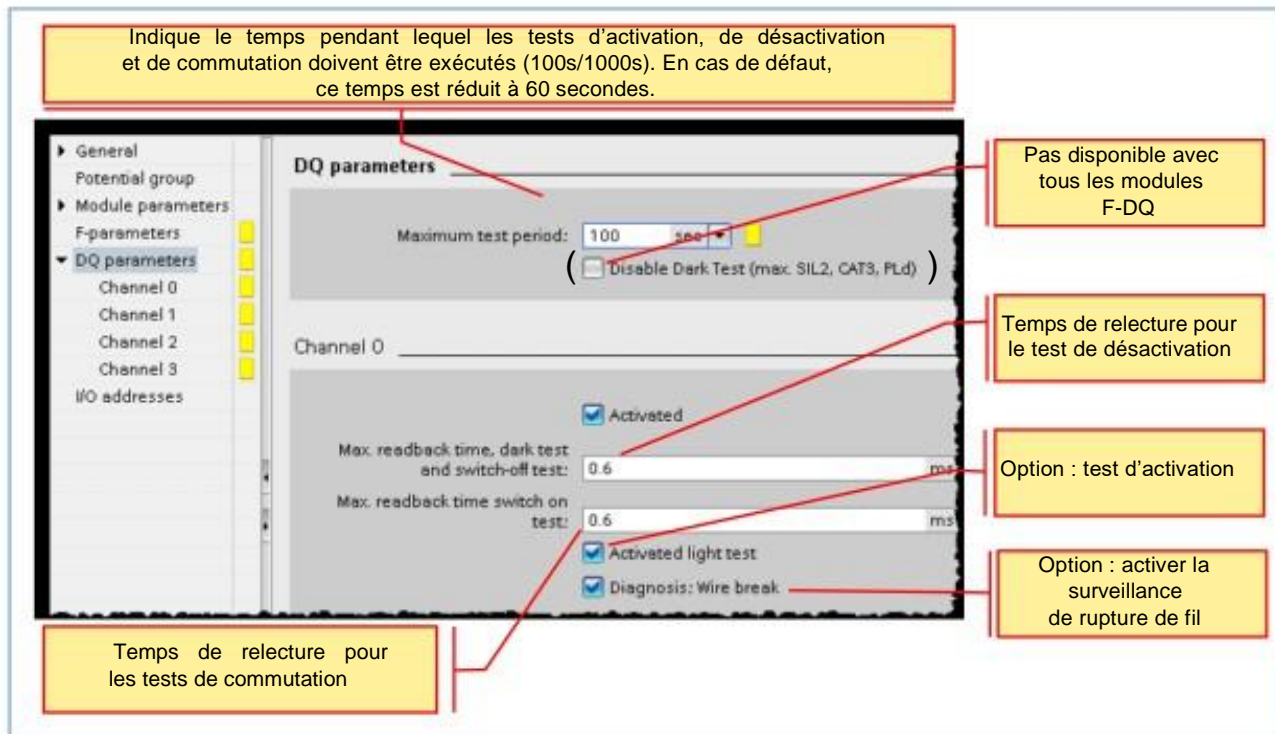
5.5. Vue d'ensemble : raccordement des actionneurs au modules

DQ-F

Raccordement d'une charge par sortie	Raccordement de deux charges par sortie
 <p>Chacune des 4 sorties TOR de sécurité est constituée d'un commutateur P (DQ-P) et d'un commutateur M (DQ-M). Vous connectez la charge entre les commutateurs P et M. Pour que la tension soit appliquée à la charge, les deux commutateurs sont toujours activés.</p>	<p>Recommandé</p>  <p>En parallèle avec P et M</p> <p>Pour maîtriser les courts-circuits transversaux entre les commutateurs P et M d'une sortie TOR de sécurité, les deux relais sont raccordés en parallèle avec P et M.</p>  <p>Raccordement à L+ et M</p> <p>Vous pouvez raccorder deux relais à une sortie TOR de sécurité. Veillez à ce qu'un même potentiel de référence soit utilisé et que les contacts de travail des deux relais soit raccordés en série.</p>

5.6. Paramètres DQ-F

5.6.1. Paramètres des canaux (1)



Temps de test maximal

Ce paramètre permet de définir la durée pendant laquelle les tests d'activation, de désactivation et de commutation (test de configuration binaire complet) doivent avoir lieu dans le module. Les tests sont répétés après l'écoulement de ce temps. En cas d'erreur, le temps de test est réduit à 60 secondes.

- Utilisez la valeur « 1000 s » pour ménager par ex. vos actionneurs.
- Utilisez la valeur « 100 s » pour détecter les erreurs plus rapidement.

Suppression du test de désactivation (max. SIL2, Cat.3, PL d)

Pour éviter une réaction indésirable de l'actionneur à un test de désactivation, vous avez la possibilité de désactiver le test de la sortie du module F. Cette réaction indésirable peut être, par exemple, un bref déclenchement d'un actionneur ou une modification de la valeur de processus d'une entrée numérique avec temps de montée court.

ATTENTION !

Pour atteindre le niveau SIL2/Cat.3/PL d, un changement de signal à la sortie correspondante de « 1 » à « 0 » doit se produire au moins une fois par an. Le signal « 0 » doit être présent pendant au moins 2 secondes. Il ne suffit pas de couper et de remettre en marche la tension d'alimentation du module F.

Activé

Si vous cochez cette case, vous activez le traitement des signaux dans le programme de sécurité pour le canal correspondant. Ce paramètre vous permet de désactiver un canal non utilisé.

Temps de relecture

C'est le temps maximal pendant lequel un signal de relecture peut encore être détecté après la coupure de la sortie avant que l'erreur « Court-circuit » n'entraîne la passivation du canal de sortie. Le temps de relecture doit, en cas de commande de charges capacitives en particulier, être paramétré à une valeur suffisamment grande pour permettre la décharge de la capacité connectée durant le temps de relecture.

Le temps de relecture est également le temps de désactivation lors d'un test de coupure. Pour vérifier le câblage de l'actionneur, des signaux 0 sont appliqués à la sortie pendant que celle-ci est active. Un actionneur doté d'une inertie suffisante ne réagit pas à la brève coupure de la sortie et reste activé.

Test d'activation

Si un signal 0 est présent à la sortie, une surcharge et une rupture de fil sont détectées. Au cours d'un test d'activation, un signal de test est appliqué sur le canal de sortie pendant que celui-ci est inactif (signal de sortie « 0 »). Le canal de sortie est alors brièvement activé (= « période d'activation ») et relu. Un actionneur possédant une inertie suffisante ne réagit pas et reste désactivé.

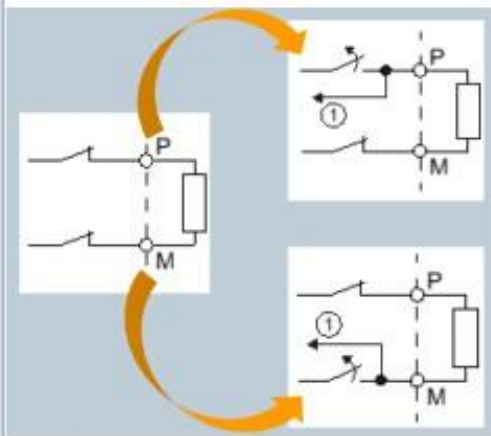
Diagnostic : Rupture de fil

Une surveillance de rupture de fil sert à la surveillance de la liaison du canal de sortie à l'actionneur. Si vous activez la case à cocher, vous activez la surveillance de rupture de fil pour le canal correspondant. Pour détecter une rupture de fil avec un signal de sortie « 0 », vous devez valider le test d'activation.

5.6.2. Test de désactivation

Test de désactivation

- Le test de désactivation fait partie du test de configuration binaire.
- Un signal de test est appliqué sur le canal de sortie pendant que celui-ci est actif (« 1 »).
- Le canal de sortie est alors brièvement désactivé (= « période de désactivation ») et relu.
- Un actionneur possédant une inertie suffisante ne réagit pas et reste activé.



Le « temps de relecture max. du test de désactivation » doit être aussi bref que possible mais suffisamment élevé pour que le canal de sortie ne soit pas passivé.

Le test de désactivation détecte les défauts suivants :

- ✓ Court-circuit entre P et L+
- ✓ Court-circuit entre M et terre
- ✓ Court-circuit transversal

① Relecture

Temps de relecture max. du test de désactivation

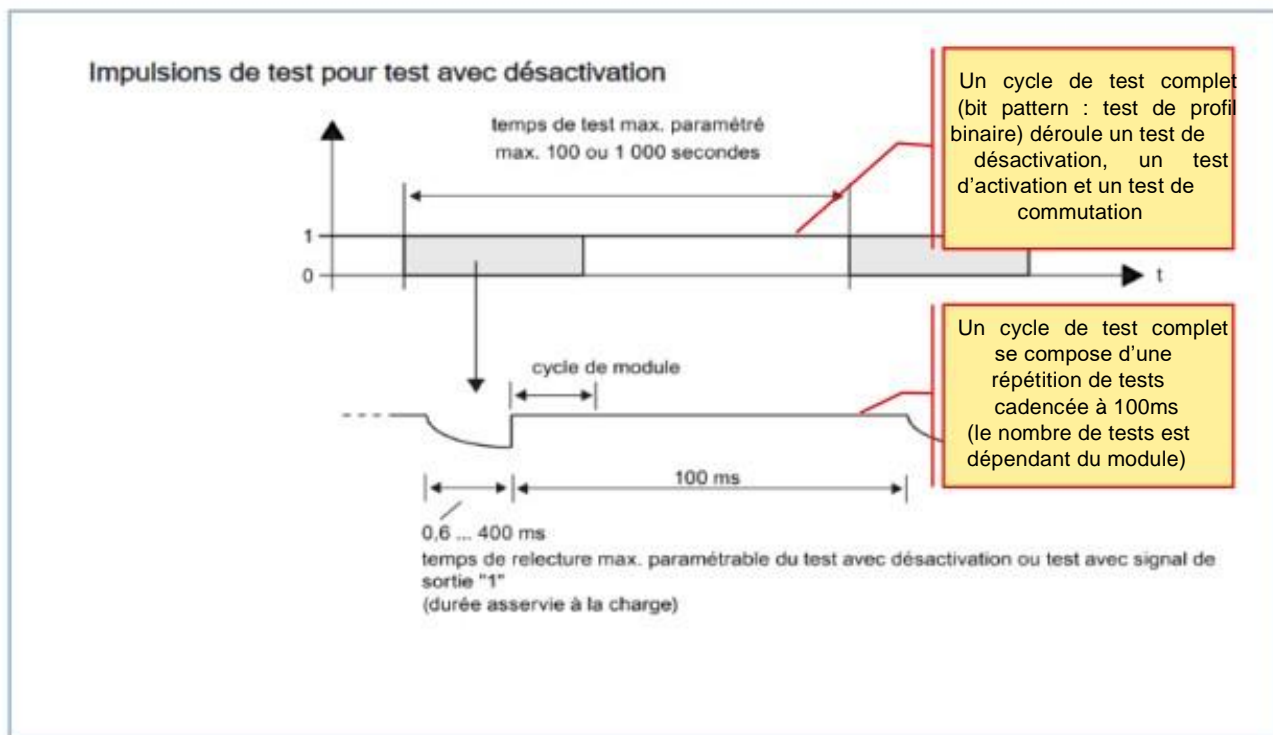
Les tests de désactivation font partie du test de configuration binaire. Lors d'un test de désactivation, un signal de test est appliqué sur le canal de sortie pendant que celui-ci est actif (signal de sortie « 1 »). Le canal de sortie est alors brièvement désactivé (= « période de désactivation ») et relu. Un actionneur possédant une inertie suffisante ne réagit pas et reste activé.

Si après écoulement du temps de relecture du test de désactivation, les signaux attendus (relecture P et M) n'ont pas pu être lus correctement, le canal de sortie est passivé. Lorsqu'une configuration binaire est active (le test du commutateur est exécuté), aucune nouvelle valeur de process n'est appliquée sur les canaux de sortie. Par conséquent, un temps de relecture max. plus élevé pour le test de désactivation augmente le temps de réaction du module F. Ce paramètre a une incidence également sur la détection d'un court-circuit (court-circuit transversal) avec signal « 1 » lors du passage du signal de sortie de « 1 » à « 0 » via le programme de sécurité.

Réglage du temps de relecture du test de désactivation

Comme le temps de relecture du test de désactivation s'ajoute au temps de réaction aux erreurs, nous vous recommandons de régler le temps de relecture par tâtonnements sur une valeur aussi brève que possible, mais cependant suffisamment élevée pour que le canal de sortie ne soit pas passivé. Calculez le temps de relecture nécessaire pour les actionneurs à l'aide du diagramme du chapitre « Commutation de charges capacitives ». Si la capacité des actionneurs n'est pas connue, il peut être nécessaire de régler par tâtonnements la valeur du temps de relecture du test de désactivation. Cela peut également être nécessaire du fait de la dispersion des composants dans l'actionneur ou d'influences extérieures.

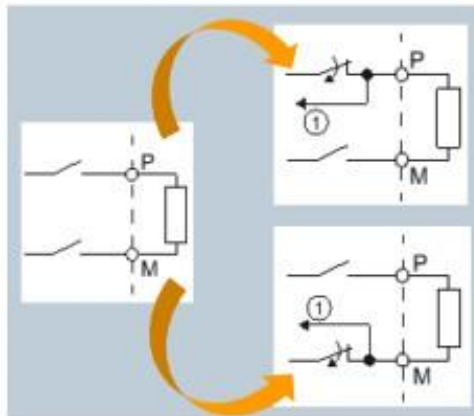
5.6.3. Allure des signaux lors du test de désactivation



5.6.4. Test de commutation

Test de commutation

- Le test de commutation fait partie du test de configuration binaire.
- Lors du test de commutation, le **commutateur P** et le **commutateur M** du canal de sortie sont **alternativement fermés** et relus lorsque le canal de sortie est inactif (« 0 »).
- Contrairement au test d'activation, aucun courant ne circule à travers la charge raccordée lors de ce test.



Le « temps de relecture max. du test de commutation » doit être aussi bref que possible mais suffisamment élevé pour que le canal de sortie ne soit pas passivé.

Le test de commutation détecte les défauts suivants :

- ✓ Court-circuit entre P et L+
- ✓ Court-circuit entre M et terre
- ✓ Court-circuit transversal

① Relecture

Temps de relecture max. du test de commutation

Le test de commutation fait partie du test de configuration binaire. Lors du test de commutation, les commutateurs P et M du canal de sortie sont alternativement fermés et relus lorsque le canal de sortie est inactif (signal de sortie « 0 »). Contrairement au test d'activation, aucun courant ne circule à travers la charge raccordée lors de ce test. Si, après écoulement du temps de relecture, le signal n'a pas pu être relu correctement, le canal de sortie est passivé.

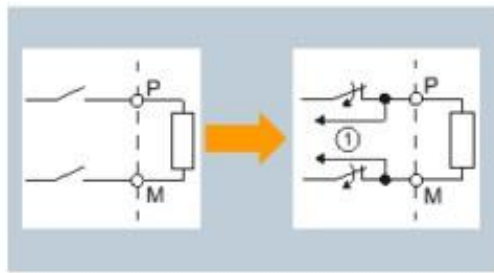
Le test de commutation détecte les défauts suivants :

- Court-circuit sur L+ avec signal de sortie « 0 »
- Court-circuit sur M avec signal de sortie « 0 »

5.6.5. Test d'activation

Test d'activation

- Un signal de test est appliqué sur le canal de sortie pendant que celui-ci est inactif (« 0 »).
- Le canal de sortie est alors brièvement activé et relu. Un actionneur possédant une inertie suffisante ne réagit pas et reste inactif.
- Contrairement au test de commutation, **les commutateurs P et M commutent simultanément** et **un courant circule à travers la charge raccordée**.



Le test d'activation détecte les défauts suivants :

- ✓ Surcharge avec signal « 0 » à la sortie
- ✓ Rupture de fil avec signal « 0 » à la sortie

① Relecture

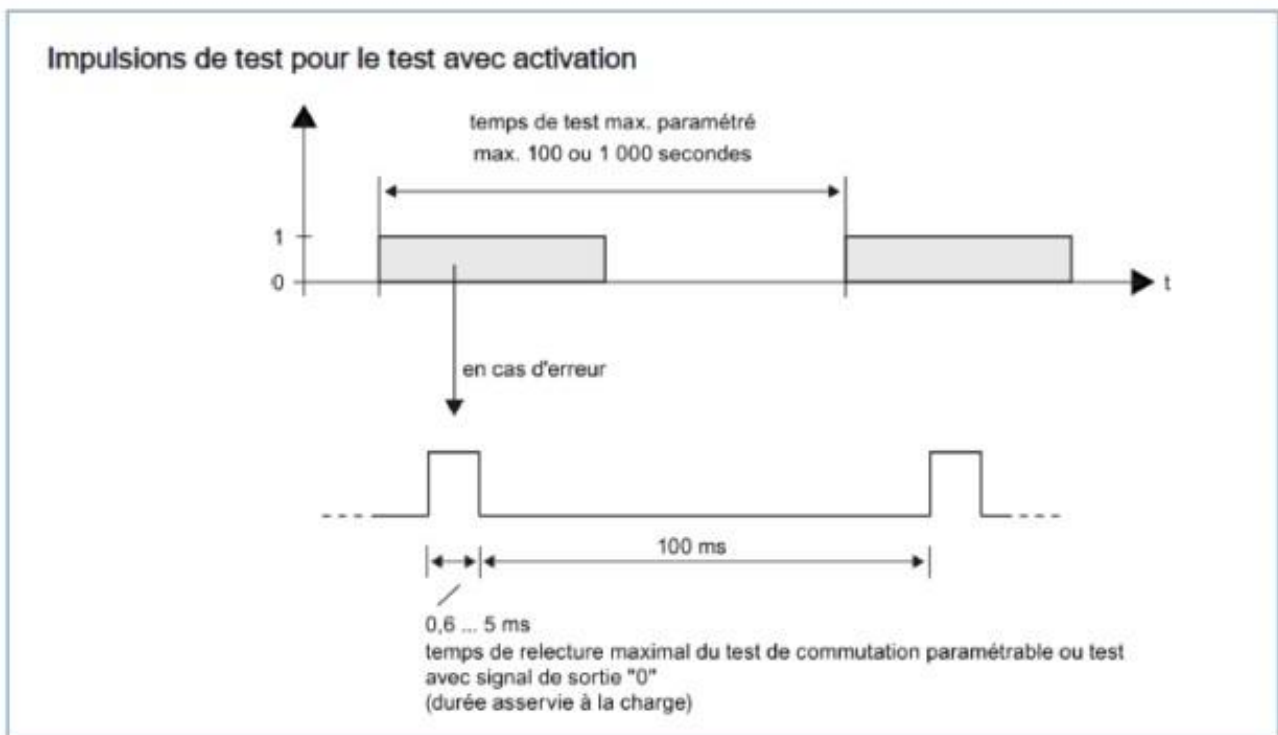
Test d'activation activé

Lors d'un test d'activation, un signal de test est appliqué sur le canal de sortie pendant que celui-ci est inactif (signal de sortie « 0 »). Le canal de sortie est alors brièvement activé (= « période d'activation ») et relu. Un actionneur possédant une inertie suffisante ne réagit pas et reste désactivé. Contrairement au test de commutation, les commutateurs P et M commutent simultanément et un courant circule à travers la charge raccordée.

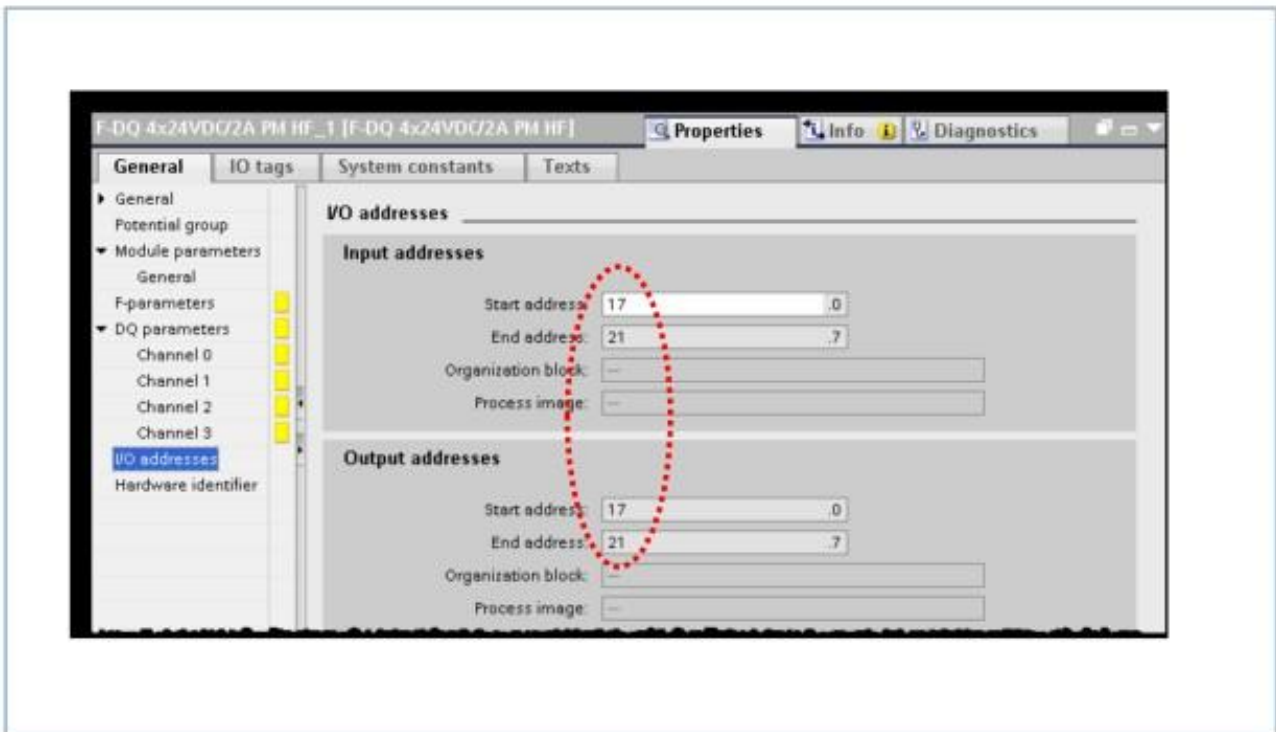
Si les signaux de relecture sont incorrects, le signal du temps de relecture paramétré est actif sur le canal de sortie avant que l'erreur n'entraîne la passivation du canal de sortie. Pendant qu'une configuration binaire est active (le test du commutateur est exécuté), aucune nouvelle valeur de process n'est appliquée sur les canaux de sortie. Par conséquent, un temps de relecture max. plus élevé pour le test d'activation augmente le temps de réaction du module.

Une impulsion d'activation de la durée paramétrée a lieu pendant le temps de test max. paramétré pour chaque canal de sortie. Si l'impulsion d'activation détecte une erreur, la même impulsion (c'est-à-dire la même configuration binaire) est répétée une fois au bout de 100 ms. Si l'erreur persiste, la durée max. du test est automatiquement raccourcie à 60 secondes et un message de diagnostic est généré. Si l'erreur a disparu, le canal de sortie est réintégré après le prochain cycle de test sans erreur.

5.6.6. Allure des signaux lors du test d'activation



5.6.7. Adresses d'E/S

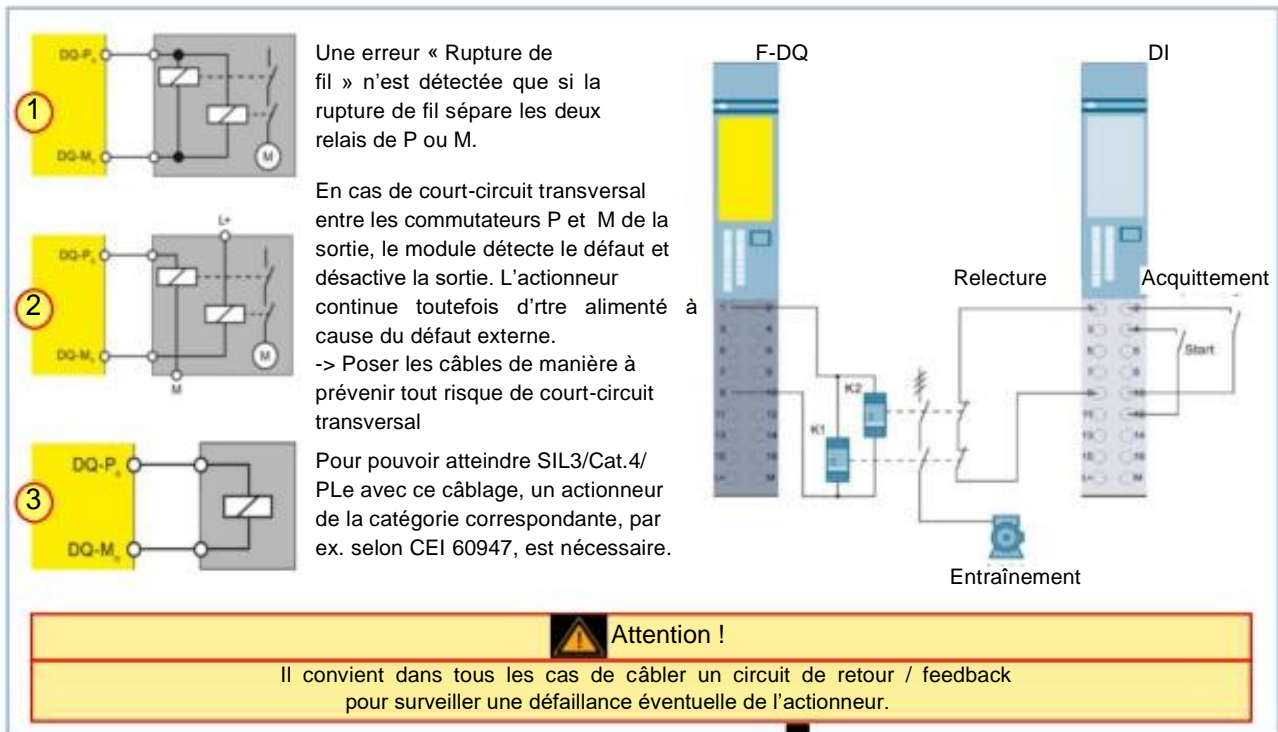


Adresses des entrées et sorties

Les adresses des modules d'entrée et sortie de sécurité sont librement paramétrables comme avec les modules standard. Pour le traitement de la communication de sécurité PROFIsafe, les modules d'entrée ou de sortie de sécurité utilisent, outre les données utiles d'entrée ou de sortie, des octets supplémentaires dans la mémoire image des entrées et des sorties. Un module F-DI occupe donc également des octets dans la mémoire image des sorties, un module F-DQ également des octets dans la mémoire image des entrées.

Vous ne pouvez accéder qu'aux adresses occupées par des données utiles et des états de valeur. Les autres zones d'adresses occupées par les modules F sont entre autres réservées à la communication de sécurité entre les modules F et la F-CPU en conformité avec PROFIsafe.

5.6.8. Exemple : raccordement d'un actionneur jusqu'à SIL3/Cat.4/PLe



Raccordement de 2 charges en parallèle par sortie TOR

Pour maîtriser les courts-circuits transversaux entre les commutateurs P et M d'une sortie de sécurité TOR, nous vous recommandons la variante de câblage en bas de la diapositive. Ce raccordement vous permet d'atteindre la classe SIL3/Cat.4/PLe.

Raccordement de charges à L+ et M par sortie TOR

Vous pouvez raccorder 2 relais sur une sortie TOR de sécurité. Tenez compte des conditions suivantes :

- Même potentiel de référence
- Les contacts de travail des deux relais doivent être branchés en série.

Ce raccordement vous permet d'atteindre la classe SIL3/Cat.4/PLe (relecture de l'état du processus nécessaire). Lors du raccordement de 2 relais à une sortie TOR (comme sur la figure ci-dessus), les défauts « Rupture de fil » et « Surcharge » sont détectés uniquement sur le commutateur P de la sortie (pas sur le commutateur M). En cas de court-circuit transversal entre les commutateurs P et M de la sortie, le module détecte le défaut et désactive la sortie. L'actionneur continue toutefois d'être alimenté à cause du défaut externe. Pour éviter les courts-circuits transversaux entre les commutateurs P et M d'une sortie TOR de sécurité, vous devez poser les câbles de raccordement des relais aux commutateurs P et M de manière à prévenir tout risque de court-circuit transversal.

Raccordement d'une charge par sortie TOR

Chacune des 4 sorties TOR de sécurité est constituée d'un commutateur P DQ-Pn et d'un commutateur M DQ-Mn. Vous raccordez la charge entre les commutateurs P et M. Les deux commutateurs sont toujours activés pour que la tension soit présente sur la charge. Ce raccordement vous permet d'atteindre la classe SIL3/Cat.4/PLe.

Évaluation des signaux de retour

Pour détecter la soudure de contacteurs, vous devez évaluer les signaux de retour ou de relecture des contacteurs dans le programme de sécurité. La bibliothèque de blocs de Safety Advanced met à cet effet un bloc certifié à votre disposition.

En cas de détection d'une erreur de relecture sur un groupe, ce dernier est désactivé. L'autre groupe peut continuer à être enclenché normalement et coupé en toute sécurité.

5.7. F-Power Module: F-PM-E 24VDC/8A PPM

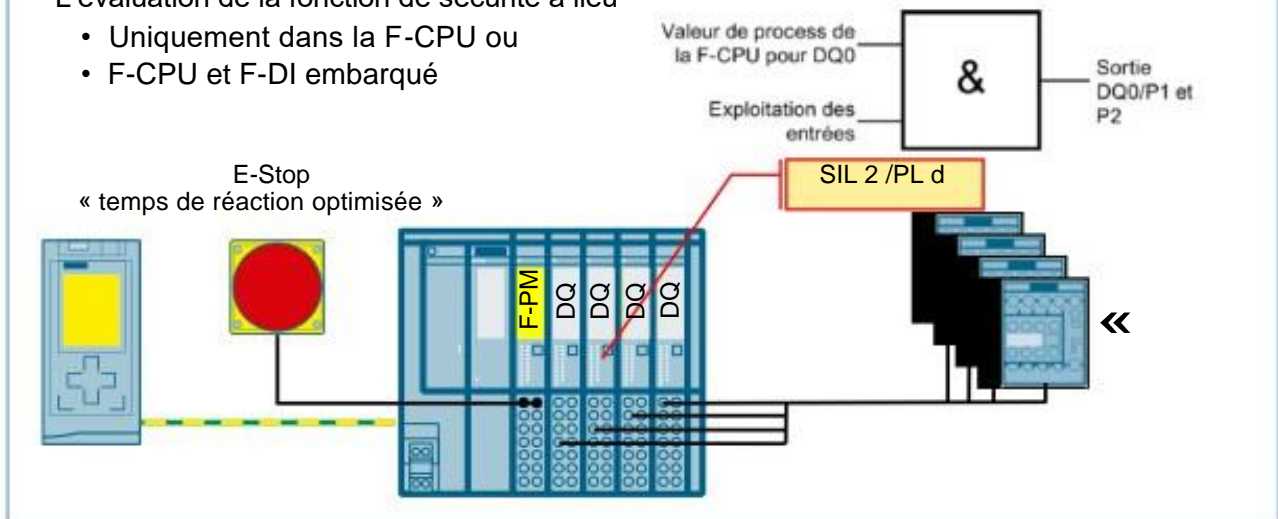
F-PM-E 24VDC/8A PPM

- 2 entrées (SIL 3/PL e)
- 1 sortie à commutation PM ou PP, courant de sortie 8 A (SIL 3/PL e)

Coupure de sécurité de modules DQ standard

L'évaluation de la fonction de sécurité a lieu

- Uniquement dans la F-CPU ou
- F-CPU et F-DI embarqué



Coupure de sécurité des modules DQ standard par le F-PM-E

Cette solution peu coûteuse vous permet de désactiver intégralement et simultanément toutes les sorties concernées des modules DQ standard en cas de détection d'erreur dans le processus ou sur le module de puissance F-PM-E 24VDC/8A PPM ST. Avec la coupure de sécurité des modules DQ standard, vous atteignez la classe SIL2/Cat.3/PLd. Vous pouvez utiliser le module de puissance F-PM-E 24VDC/8A PPM ST avec tous les modules standard DQ à l'intérieur d'un groupe de potentiel.

Sortie TOR de F-PM

La sortie TOR commute la tension entre L+ et M via deux commutateurs électroniques. La tension commutée et la masse sont transmises via les barres de potentiel internes P1 et P2. La tension commutée et la masse sont en outre disponibles sur la BaseUnit aux sorties DQ-P0 et DQ-M0.

Vous disposez ainsi de deux possibilités de raccordement, que vous pouvez par ailleurs utiliser simultanément :

- Une charge peut être directement raccordée à la BaseUnit.
- Les barres de potentiel internes P1 et P2 permettent d'alimenter des modules standard et de réaliser une coupure de sécurité. Vous pouvez également raccorder des charges aux modules standard.

En cas de court-circuit transversal entre L+ et DQ, l'actionneur commandé n'est plus désactivé. Pour éviter les courts-circuits transversaux entre L+ et DQ, vous devez poser les câbles de raccordement des actionneurs de manière à prévenir tout risque de court-circuit transversal (par ex. câbles à gaines séparées ou placés dans des goulottes séparées). Avec le module F-PM-E, vous devez, pour des raisons de sécurité, poser un câble de masse double vers la BaseUnit. Sinon, la barre de potentiel P2 ne pourrait plus être désactivée de manière sûre en cas de rupture d'un câble de masse simple.

5.8. PM-F Paramètres des canaux

L'évaluation de la fonction de sécurité peut être réalisée dans la « F-CPU » ou la « F-CPU et F-DI embarqué » pour une coupure de groupe rapide.

Indique si la sortie est à commutation PM ou PP

Commutation PM

Commutation PP

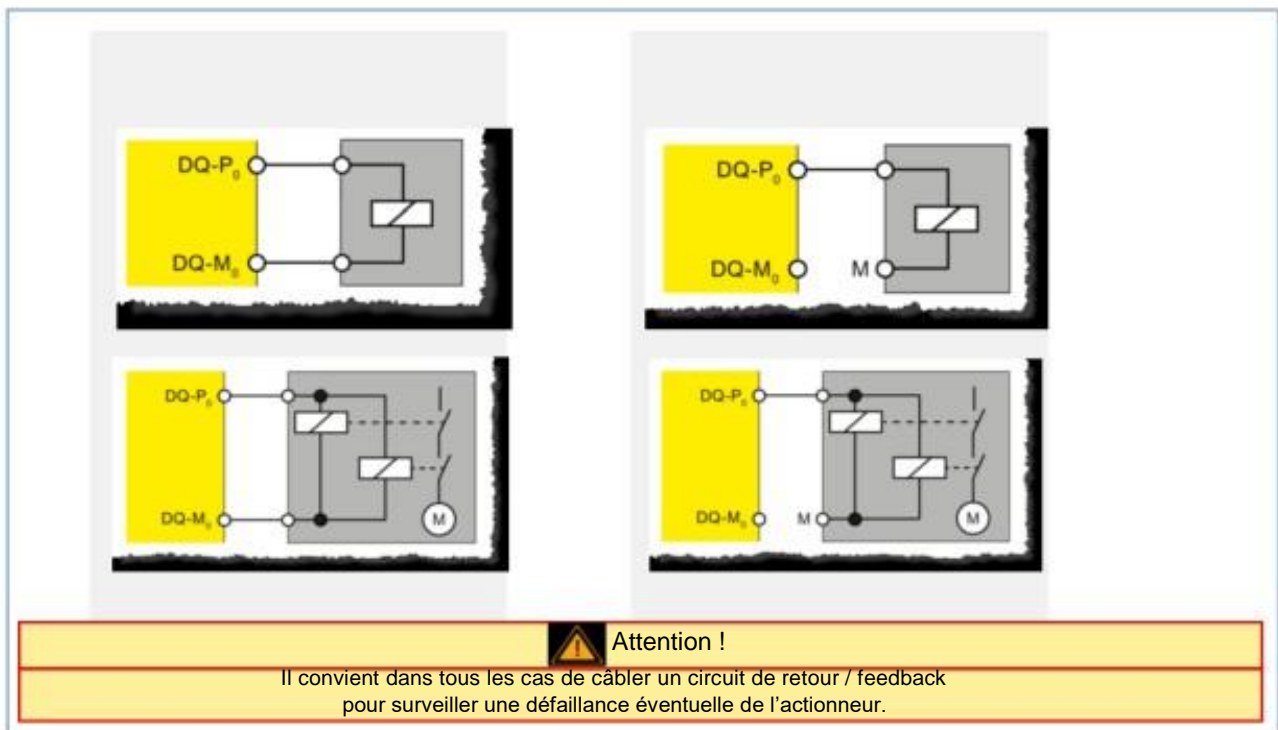
Coupure de sécurité des modules de sortie standard, commutation PM

Le module de puissance F-PM-E 24VDC/8A PPM ST ouvre un nouveau groupe de potentiel avec la BaseUnit appropriée. Les modules DQ standard utilisés dans ce groupe de potentiel peuvent être désactivés de manière sécurisée par le module de puissance F-PM-E 24VDC/8A PPM ST. Pour ce faire, le module de puissance F-PM-E 24VDC/8A PPM ST désactive les barres de potentiel P1 et P2 de manière sécurisée.

Coupure de sécurité des modules de sortie standard, commutation PP

Le module de puissance F-PM-E 24VDC/8A PPM ST ouvre un nouveau groupe de potentiel avec la BaseUnit appropriée. Les modules DQ standard utilisés dans ce groupe de potentiel peuvent être désactivés de manière sécurisée par le module de puissance F-PM-E 24VDC/8A PPM ST. Pour ce faire, le module de puissance F-PM-E 24VDC/8A PPM ST désactive les barres de potentiel P1 de manière sécurisée.

5.9. PM-F Raccordement d'un actionneur : commutation PM / PP



Raccordement d'une charge à la sortie TOR, commutation PP (voir vue en haut à droite)

La sortie TOR de sécurité se compose de deux commutateurs P pour DQ-P0 et d'un commutateur M pour DQ-M0. Vous raccordez dans ce cas la charge entre le commutateur P DQ-P0 et la masse. Pour que la tension soit présente sur la charge, les deux commutateurs P sont toujours activés. Ce raccordement vous permet d'atteindre la classe SIL3/Cat.4/PLe avec un actionneur de la catégorie correspondante.

Raccordement d'une charge à la sortie TOR, commutation PM (voir vue en haut à gauche)

La sortie TOR de sécurité se compose de deux commutateurs P pour DQ-P0 et d'un commutateur M pour DQ-M0. Vous raccordez dans ce cas la charge entre les commutateurs P DQ-P0 et le commutateur M DQ-M0. Pour que la tension soit présente sur la charge, les deux commutateurs P et le commutateur M sont toujours activés. Ce raccordement vous permet également d'atteindre la classe SIL3/Cat.4/PLe avec un actionneur de la catégorie correspondante.

Raccordement de 2 charges en parallèle à la sortie TOR, commutation PP

Avec la variante de câblage représentée en bas à droite de la diapositive, vous pouvez atteindre la classe SIL3/Cat.4/PLe. Le raccordement en parallèle de 2 relais obéit aux mêmes règles qu'un raccordement avec commutation PM.

Raccordement de 2 charges en parallèle à la sortie TOR, commutation PM

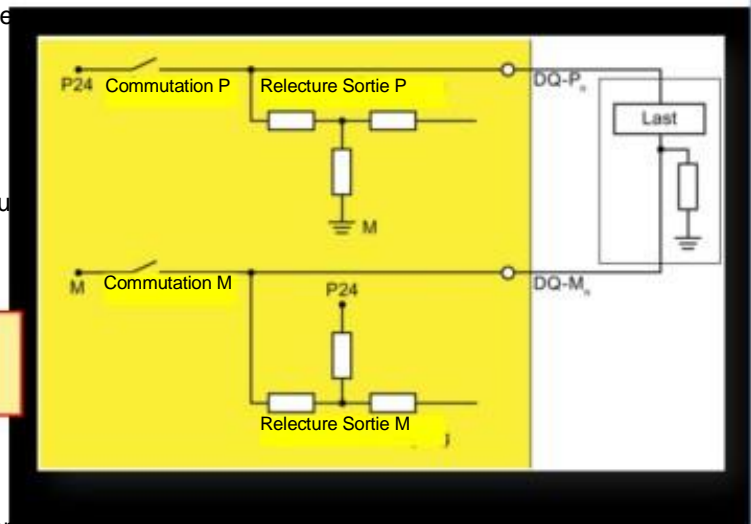
Avec la variante de câblage représentée en bas à gauche de la diapositive, vous pouvez atteindre la classe SIL3/Cat.4/PLe. Lors d'un raccordement en parallèle de 2 relais à une sortie TOR, une rupture de fil n'est détectée que si les deux relais sont séparés de P ou M par cette rupture de fil. Le diagnostic alors généré n'est pas significatif pour la sécurité.

5.9.1. Commutation de charges avec liaison à la terre

Un module PM détecte un court circuit si les de

- Commutation de charge qui présente une liaison entre la masse et la terre pour améliorer la tenue CEM.
- Si les masse et la terre sont confondues au niveau de l'alimentation.

Du point de vue du module F, le commutateur M est ponté par la connexion masse-terre.



Remède:

- Réduire la capacité entre la masse et la terre au niveau de la charge à une valeur inférieure à $2\mu F$.
- Augmenter la valeur de la résistance entre la masse et la terre pour dépasser 100 k Ω .

OU

- Utilisez un module à commutation PP.

F-DQ à commutation PP

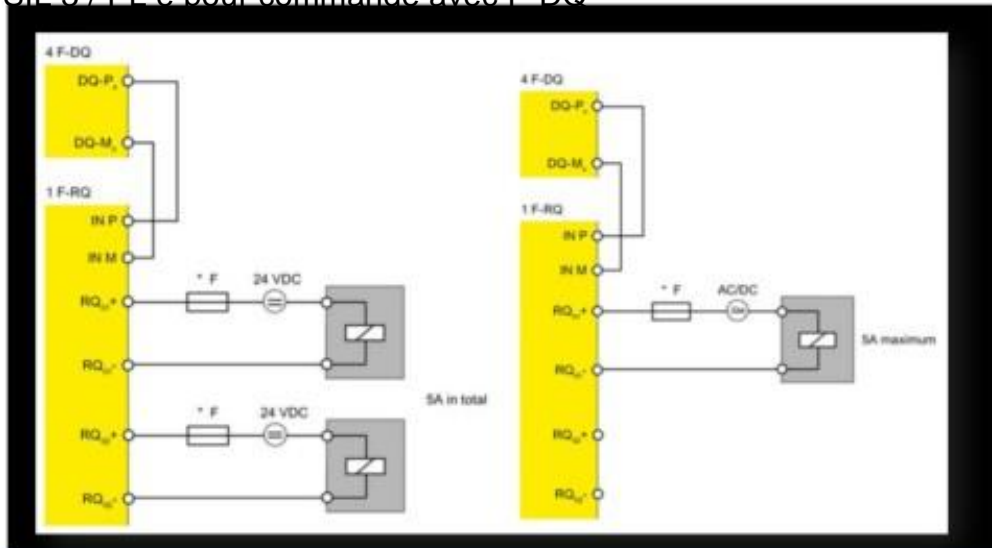
Un module F-DQ à commutation PM détecte un court-circuit si des charges comportant une liaison entre masse et terre (par ex. pour améliorer la CEM) sont commutées et si la masse et la terre sont reliées lorsque le bloc d'alimentation fournit de l'énergie. Du point de vue du module F, cette liaison masse-terre court-circuite le commutateur M. Un module F-DQ à commutation PP peut constituer une solution.

5.10. Module à relais F : F-RQ 1x24VDC/24...230VAC/5A

Coupure séparée électriquement avec :

ET 200SP 1 F-RQ

- 1 sortie relais (2x contacts à fermeture 2 canaux)
- SIL 3 / PL e pour commande avec F-DQ



Coupure unipolaire de charges

Dans ce cas d'application, vous pouvez effectuer, avec un module F-RQ, une commutation unipolaire de deux charges avec 5 A au total et une/deux alimentations TBTS/TBTP.

Coupure bipolaire d'une charge avec 1 module F-RQ

Dans ce cas d'application, vous pouvez effectuer, avec un module F-RQ, une commutation bipolaire d'une charge avec 2,5 A max. et une alimentation TBTS/TBTP.

Coupure bipolaire d'une charge avec 2 modules F-RQ

Dans ce cas d'application, vous pouvez effectuer, avec 2 modules F-RQ, une commutation bipolaire d'une charge avec max. 5 A.

Coupure unipolaire de charges avec 2 modules F-RQ

Dans ce cas d'application, vous pouvez effectuer, avec 2 modules F-RQ, une commutation unipolaire de deux charges de 5 A chacune. L'alimentation n'est pas une TBTS/TBTP.

5.11. Commutation du module à relais F avec DQ-F

Structure interne

- Signal de retour interne au module via mémoire image :

Schéma de principe

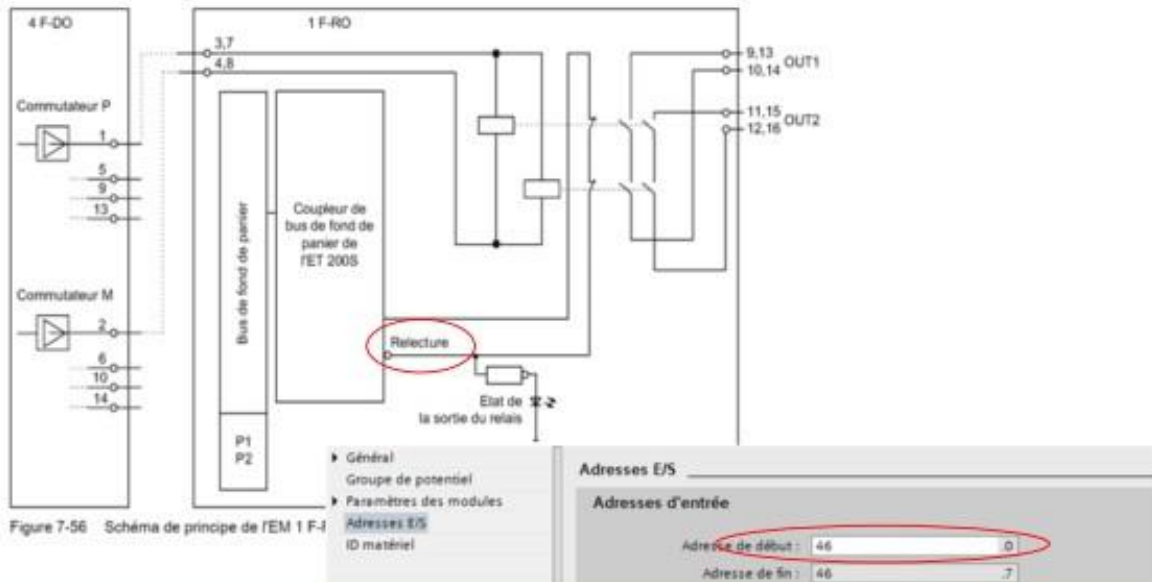


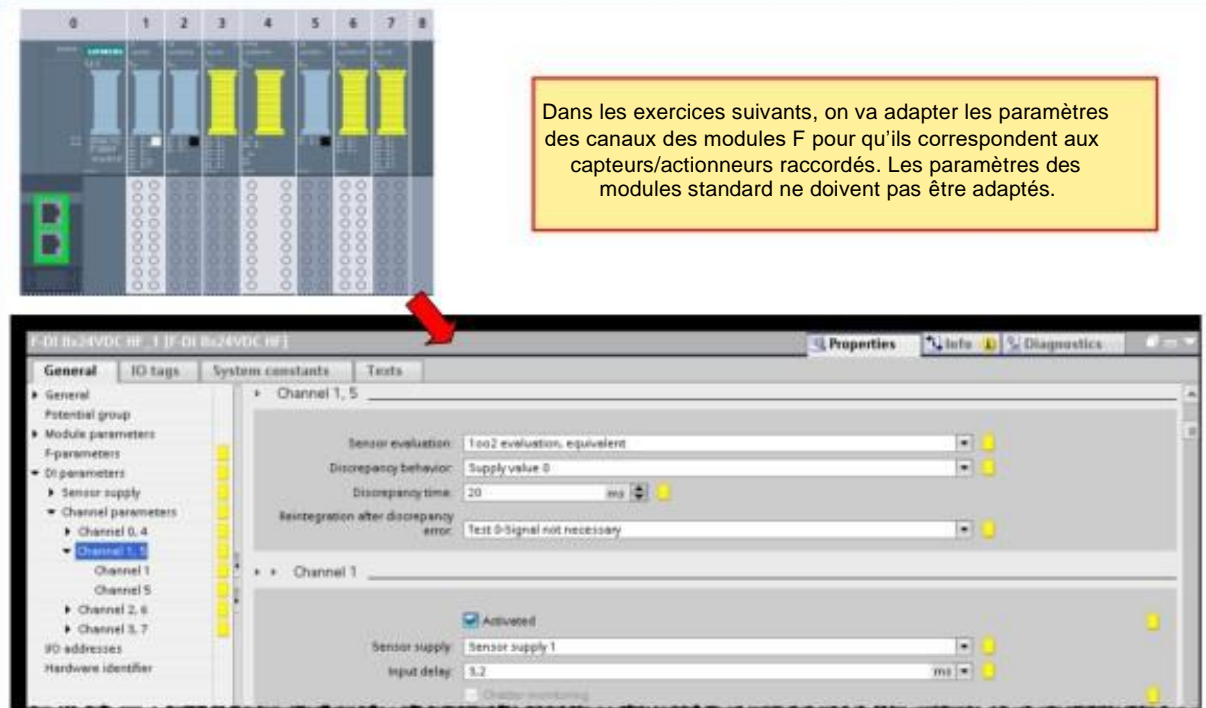
Figure 7-56 Schéma de principe de l'EM 1 F-I

Raccordement de l'alimentation 24 V DC

Appliquez la tension de commande 24 V DC à IN P (borne 9) et IN M (borne 11). L'alimentation 24 V DC s'effectue généralement via une sortie de sécurité à commutation PM (par ex. module de sortie TOR F-DQ 4x24VDC/2A PM HF). Raccordez la sortie P de F-DQ à IN P du module F-RQ et la sortie M à IN M du module F-RQ.

Le raccordement à une sortie de sécurité à commutation PP est également possible. Notez toutefois que les courts-circuits P externes sur l'entrée P ne peuvent pas être maîtrisés. IN M serait dans ce cas directement relié à la masse de la tension de commande. L'intervention de la tension de commande aux entrées IN P et IN M entraîne la destruction du module F-RQ.

5.12. Énoncé : Adapter les paramètres des modules F



The image shows a screenshot of the SIMATIC TIA Portal interface. At the top, a hardware rack is displayed with modules 0 through 8. Modules 3, 4, 5, and 6 are highlighted in yellow. A red arrow points from module 5 in the rack to the 'Properties' window below. The 'Properties' window is titled 'F-DI 16xDC nr. 1 [F-DI 16xDC nr. 1]' and has tabs for 'General', 'IO tags', 'System constants', and 'Texts'. The 'General' tab is selected, showing parameters for 'Channel 1, 5'. The parameters are:

- Sensor evaluation: 1oo2 evaluation, equivalent
- Discrepancy behavior: Supply value 0
- Discrepancy time: 20 ms
- Reintegration after discrepancy error: Test 0-Signal not necessary

Below these, there is a section for 'Channel 1' with the following parameters:

- Activated: ☒
- Sensor supply: Sensor supply 1
- Input delay: 3.2 ms
- Channel monitoring: ☐

A yellow box with a red border contains the following text:

Dans les exercices suivants, on va adapter les paramètres des canaux des modules F pour qu'ils correspondent aux capteurs/actionneurs raccordés. Les paramètres des modules standard ne doivent pas être adaptés.

5.13. Exercice 1 : Paramétrage F-DI, emplacement 3

Arrêt d'urgence E2 :
un interrupteur 2 canaux
avec évaluation 1oo2
et une alimentation capteurs
interne raccordés

Interrupteur de maintenance :
2 interrupteurs un canal avec évaluation 1oo1
et alimentation capteurs interne raccordés

Arrêt d'urgence E1 :
un interrupteur 2 canaux
avec évaluation 1oo2
et alimentation capteurs
interne raccordés

Paire de canaux 3,7

Canal 0

Canal 4

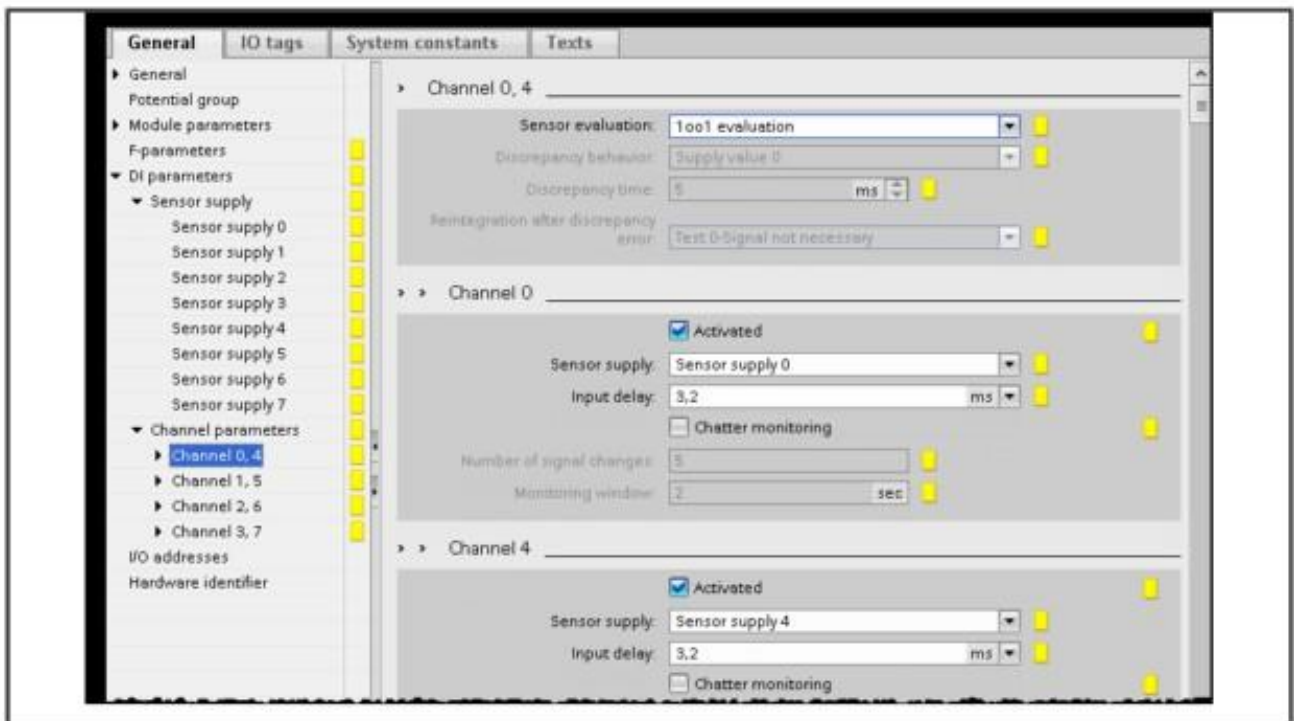
Paire de canaux 1,5

La paire de canaux 2, 6 n'est pas utilisée. Les canaux 2 et 6 peuvent donc être désactivés

Énoncé et procédure

1. Ouvrez les paramètres des canaux du module F-DI à l'emplacement 3

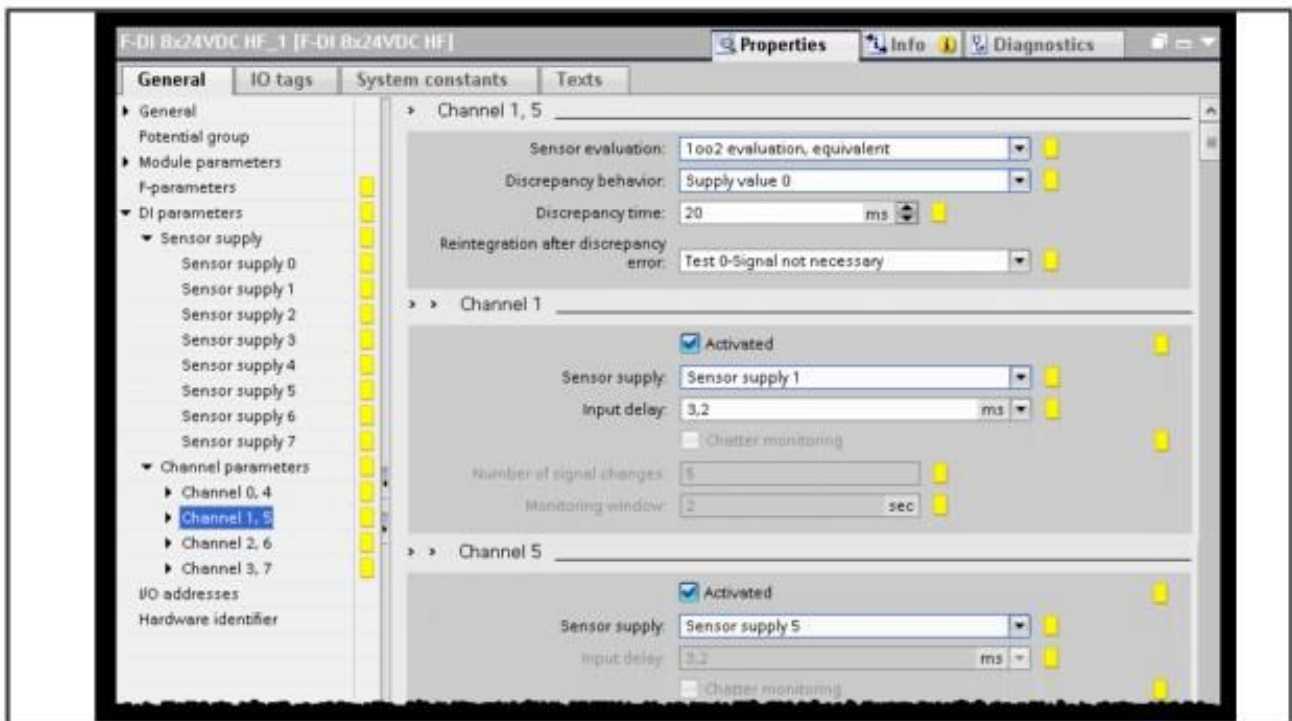
5.13.1. Exercice 1 (suite) : Interrupteur de maintenance, canal 0, 4



Énoncé et procédure

1. Paramétrez la paire de canaux 0, 4 comme indiqué sur la vue

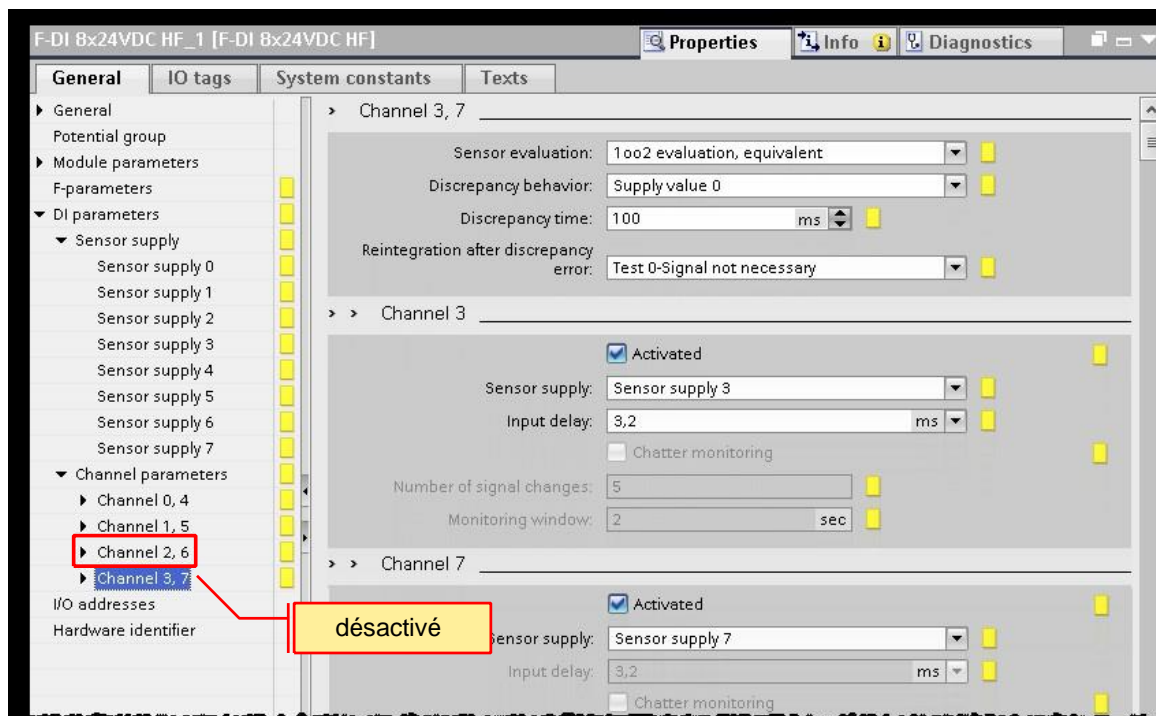
5.13.2. Exercice 1 (suite) : Arrêt d'urgence E1, canal 1,5



Énoncé et procédure

1. Paramétrez la paire de canaux 1, 5 comme indiqué sur la vue

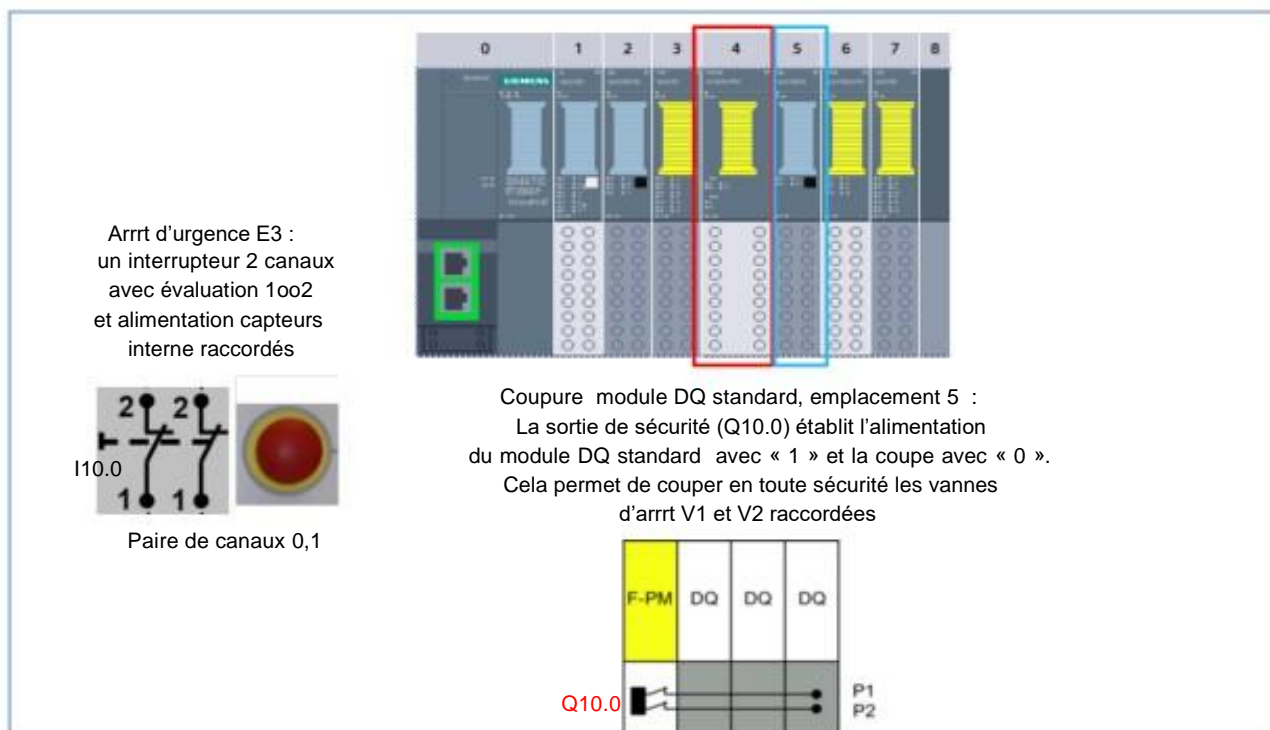
5.13.3. Exercice 1 (suite) : Arrêt d'urgence E2, canal 3, 7



Énoncé et procédure

1. Paramétrez la paire de canaux 3, 7 comme indiqué sur la vue
2. Désactivez la paire de canaux 2, 6

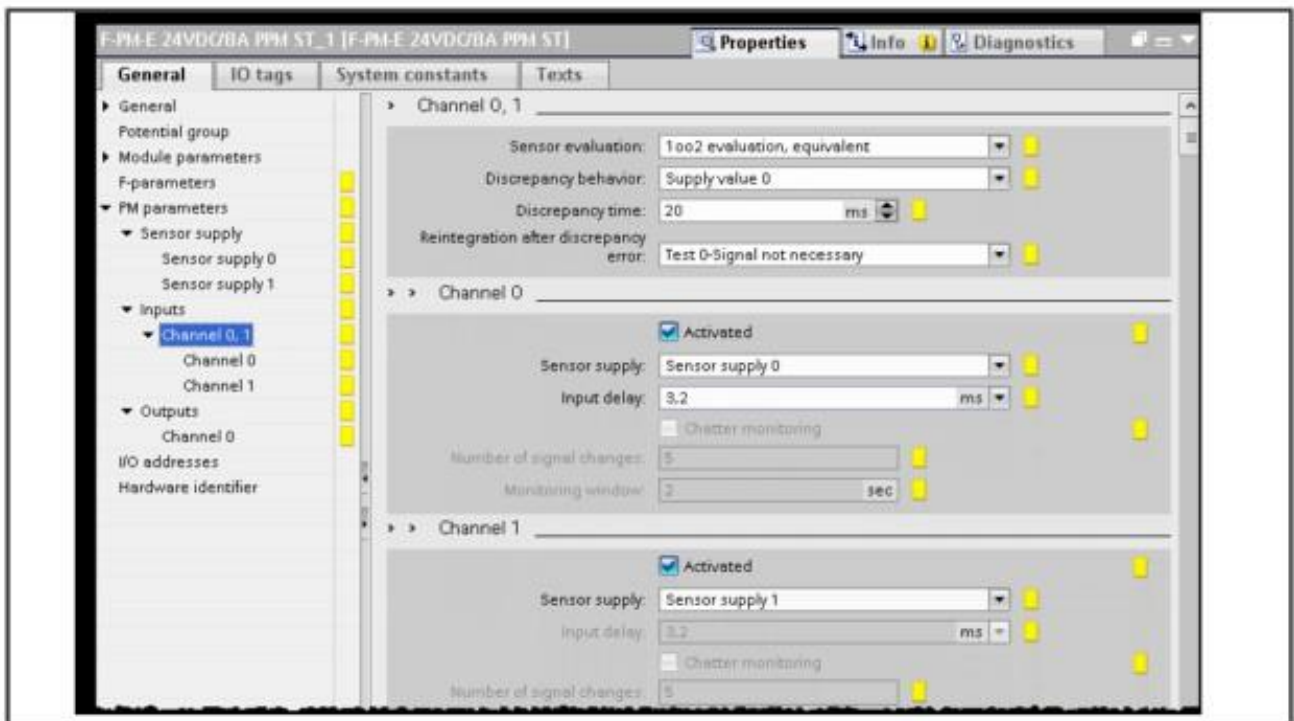
5.14. Exercice 2 : Paramétrage F-PM, emplacement 4



Énoncé et procédure

1. Ouvrez les paramètres des canaux du module F-PM à l'emplacement 4

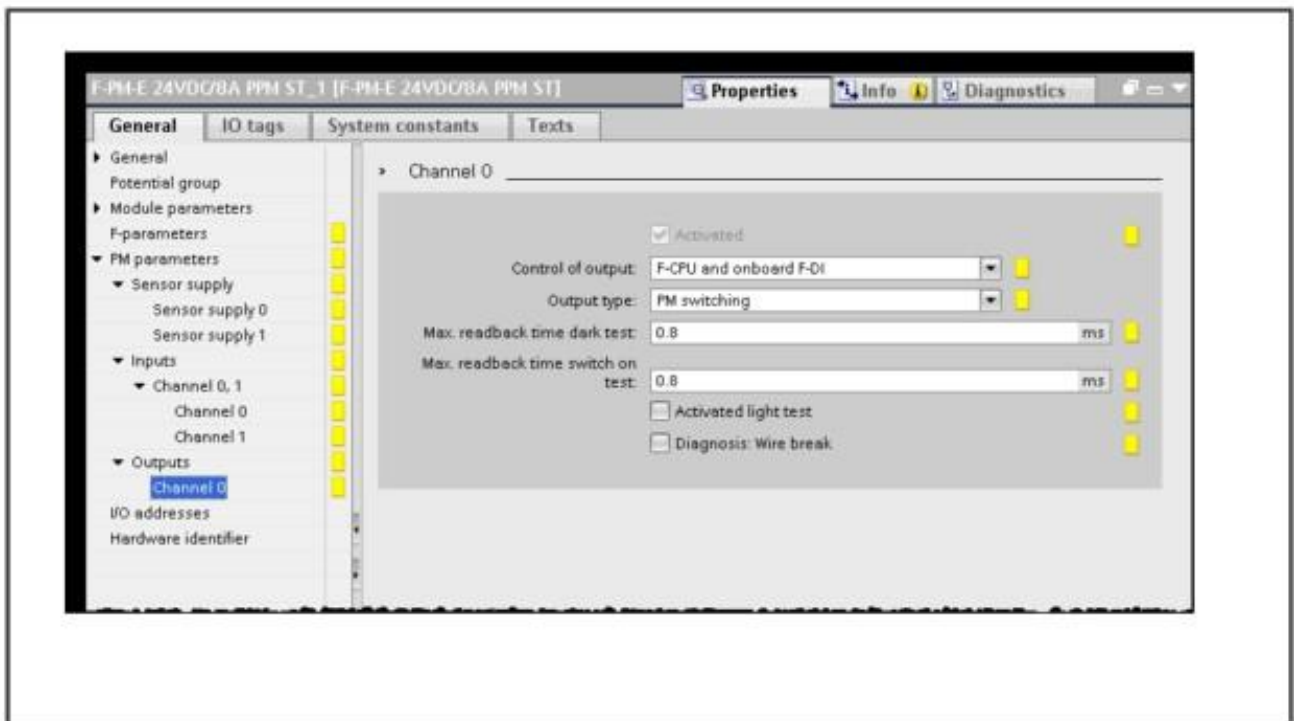
5.14.1. Exercice 2 (suite) : Arrêt d'urgence E3, canal 0, 1



Énoncé et procédure

1. Paramétrez la paire de canaux d'entrée 0, 1 comme indiqué sur la vue

5.14.2. Exercice 2 (suite) : Coupure DQ standard, canal 0

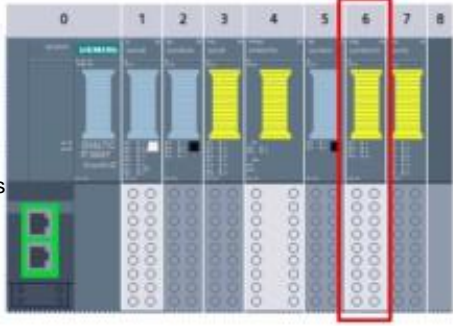


Énoncé et procédure


1. Paramétrez le canal de sortie 0 comme indiqué sur la vue

5.15. Exercice 3 : Paramétrage F-DQ, emplacement 6

Moteur M1 :
Les 2 contacteurs sont commandés en parallèle via la sortie de sécurité 0 (Q17.0).
Les signaux de retour sont relus à l'entrée standard I2.2.

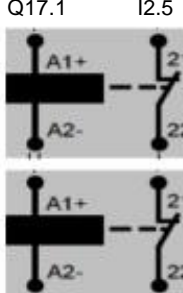


Moteur M2 :
Les 2 contacteurs sont commandés en parallèle via la sortie de sécurité 1 (Q17.1).
Les signaux de retour sont relus à l'entrée standard I2.5.

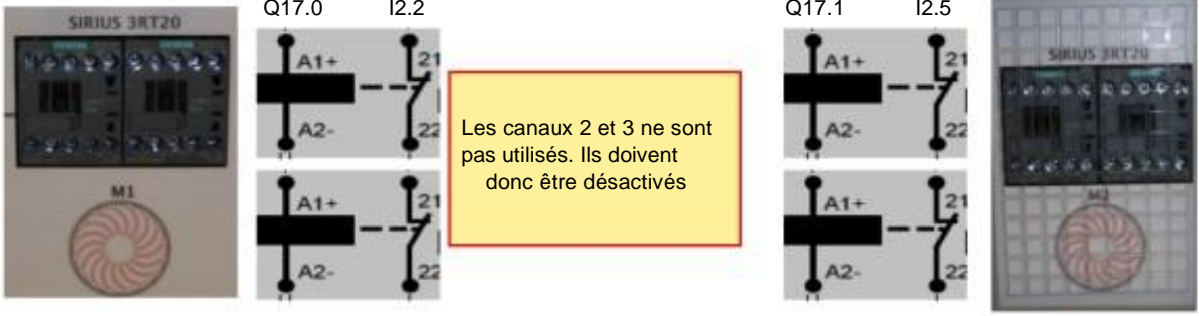


Q17.0 I2.2

Les canaux 2 et 3 ne sont pas utilisés. Ils doivent donc être désactivés



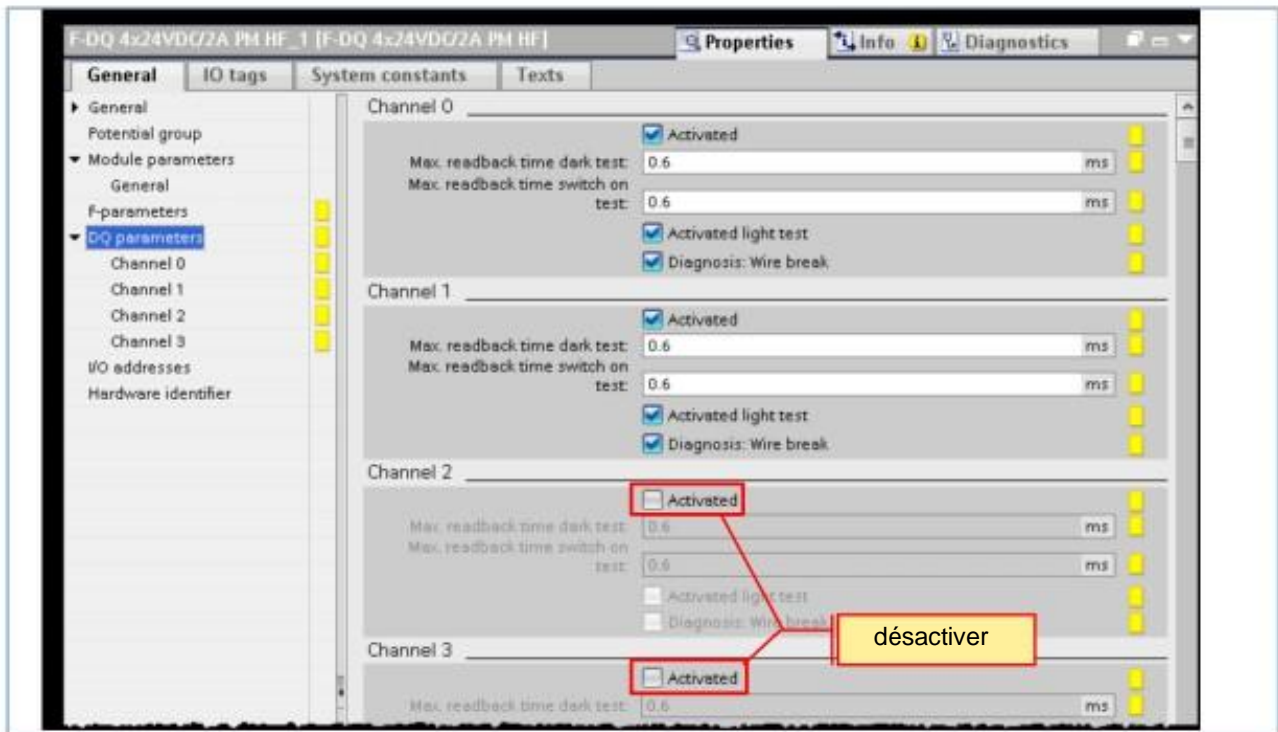
Q17.1 I2.5



Énoncé et procédure

Ouvrez les paramètres des canaux du module F-DQ à l'emplacement 6

5.15.1. Exercice 3 (suite) : Commande Moteur 1 et Moteur 2, canal 0, 1

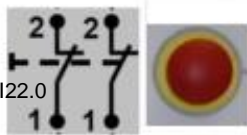


Énoncé et procédure

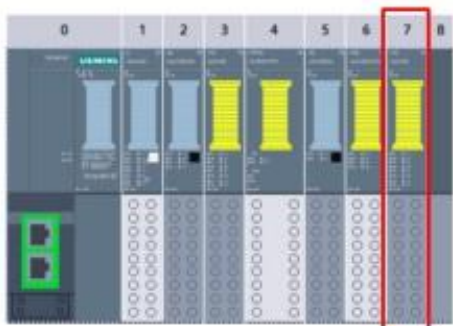
1. Paramétrez les canaux de sortie 0 et 1 comme indiqué sur la vue
2. Désactivez les canaux 2 et 3

5.16. Exercice 4 : Paramétrage F-DI, emplacement 7

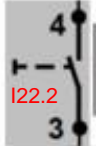
Arrêt d'urgence E4 :
un interrupteur 2 canaux
avec évaluation 1oo2
et alimentation capteurs
interne raccordée




Paire de canaux 0,4



Commande bimanuelle :
2 interrupteurs un canal avec évaluation 1oo1
et alimentation capteurs interne raccordée

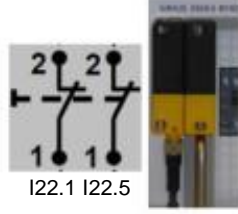


Canal 2



Canal 6

Surveillance de porte de protection :
interrupteur de sécurité RFID 2 canaux
avec évaluation 1oo1 et alimentation
capteurs externe raccordée



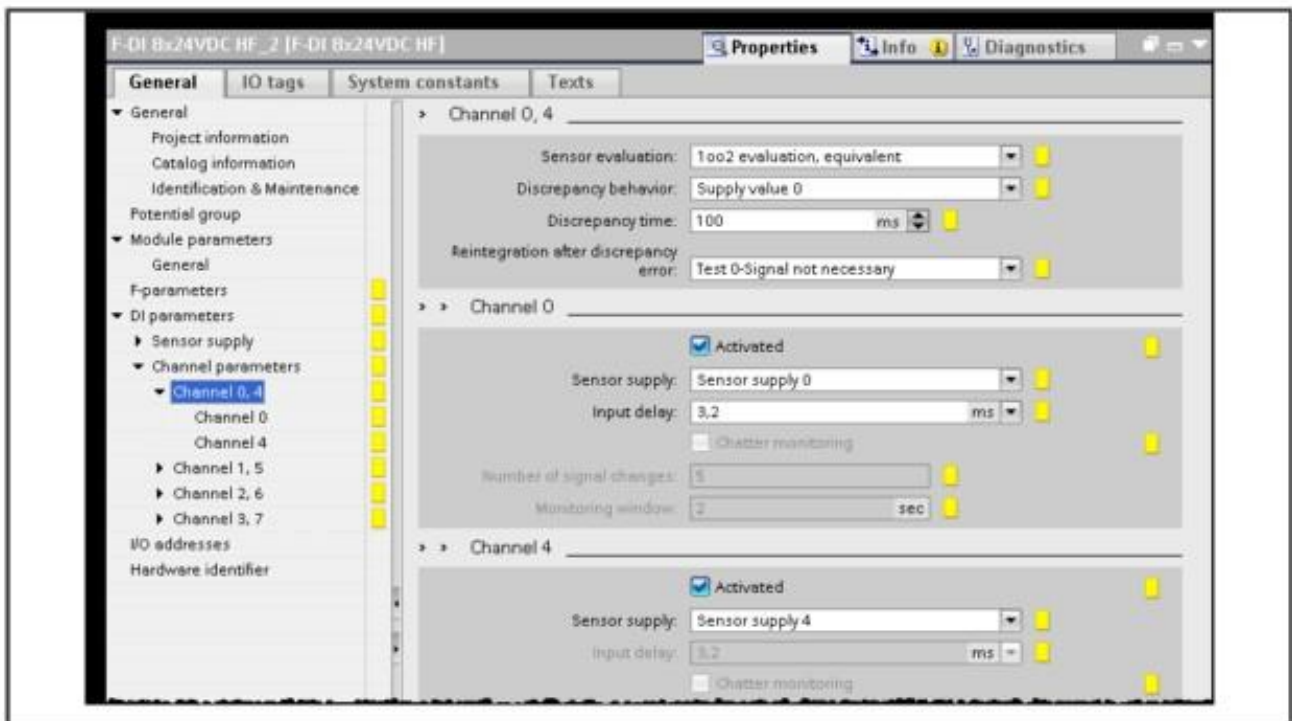
Paire de canaux 1,5

La paire de canaux 3, 7 n'est pas utilisée. Les canaux 3 et 7 peuvent donc être désactivés

Énoncé et procédure

Ouvrez les paramètres des canaux du module F-DI à l'emplacement 7

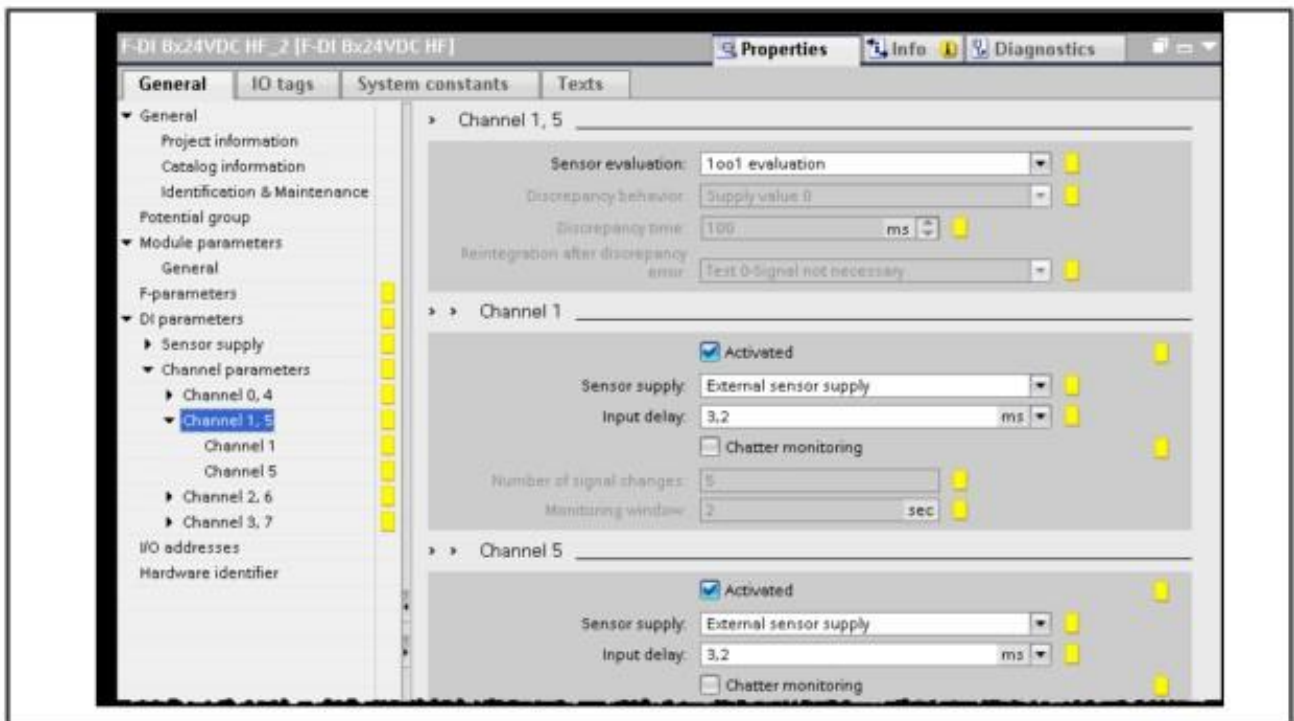
5.16.1. Exercice 4 (suite) : Arrêt d'urgence E4, canal 0,4



Énoncé et procédure

- Paramétrez la paire de canaux d'entrée 0, 4 comme indiqué sur la vue

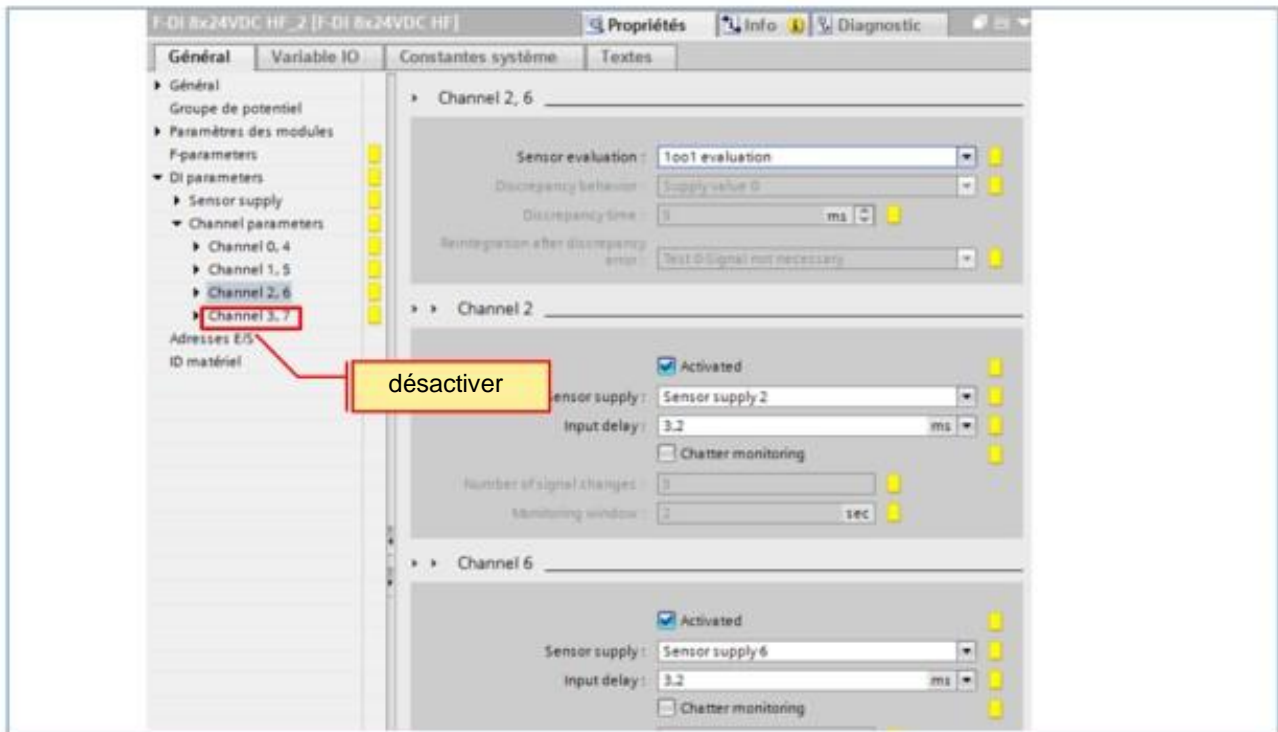
5.16.2. Exercice 4 (suite) : Interrupteur de sécurité RFID, canal 1,5



Énoncé et procédure

1. Paramétrez la paire de canaux d'entrée 1, 5 comme indiqué sur la vue

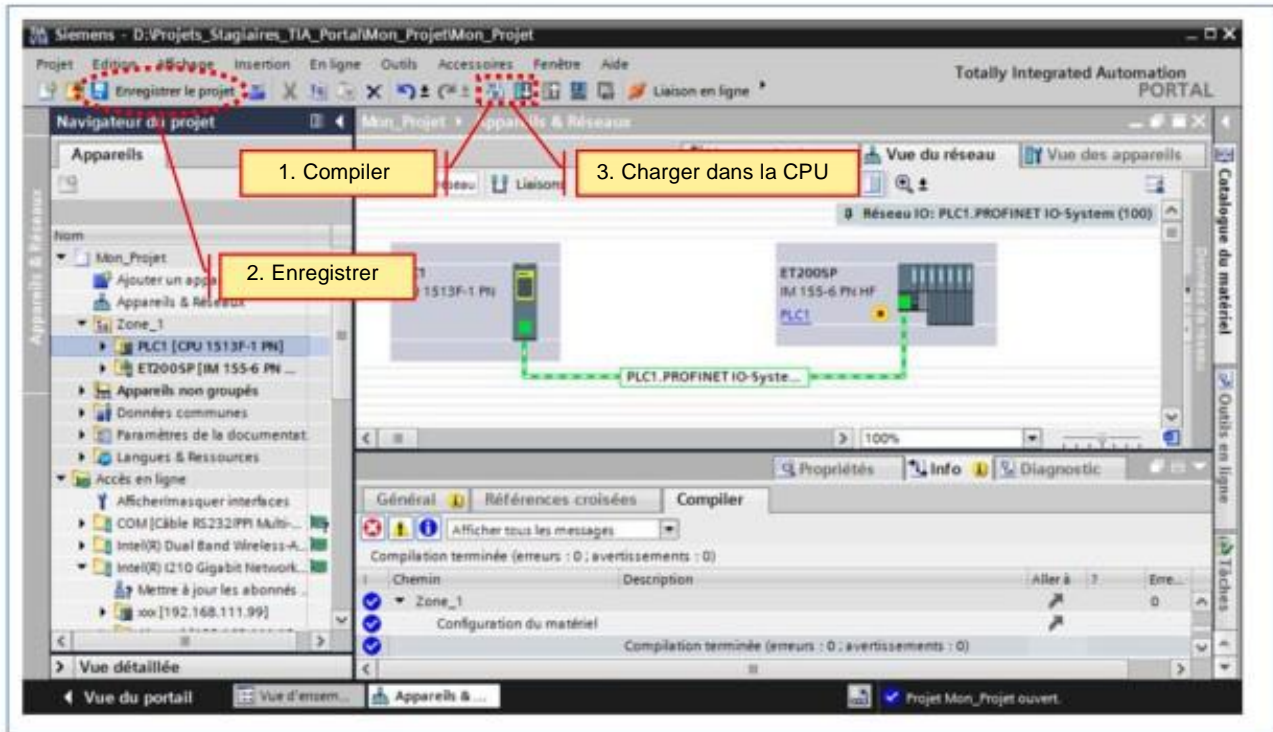
5.16.3. Exercice 4 (suite) : Surveillance commande bimanuelle, canal 2, 6



Énoncé et procédure

1. Paramétrez la paire de canaux d'entrée 2, 6 comme indiqué sur la vue
2. Désactivez la paire de canaux 3, 7

5.17. Exercice 5 : Compiler la configuration matérielle et la charger dans la CPU



Énoncé

Une fois le système d'E/S PROFINET entièrement configuré et paramétré, le projet complet doit être compilé, enregistré et chargé dans la CPU.

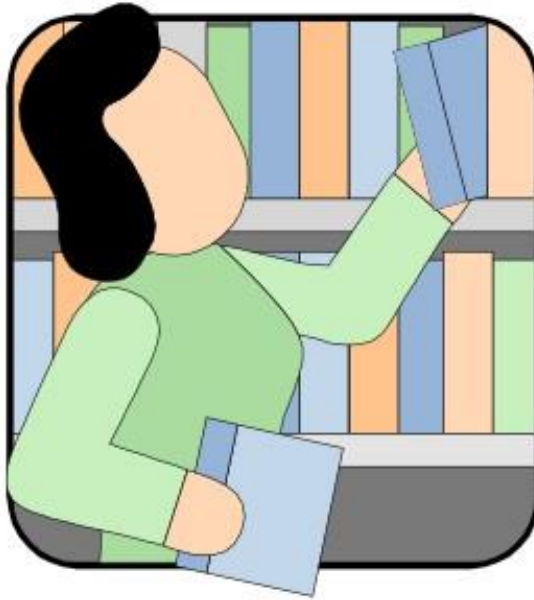
Procédure

1. Compilez la configuration matérielle en sélectionnant la station S7-1500 dans le navigateur du projet, puis en cliquant sur le bouton Compiler (voir diapositive). Vérifiez dans la fenêtre d'inspection sous « Info » si la compilation a été réalisée avec succès. Si des erreurs sont apparues, corrigez-les.
2. Enregistrez votre projet
3. Chargez la station complète dans la CPU en cliquant sur le bouton Charger (voir diapositive). Vérifiez dans la fenêtre d'inspection sous « Info » si le chargement a été réalisé avec succès.
4. Enregistrez votre projet.

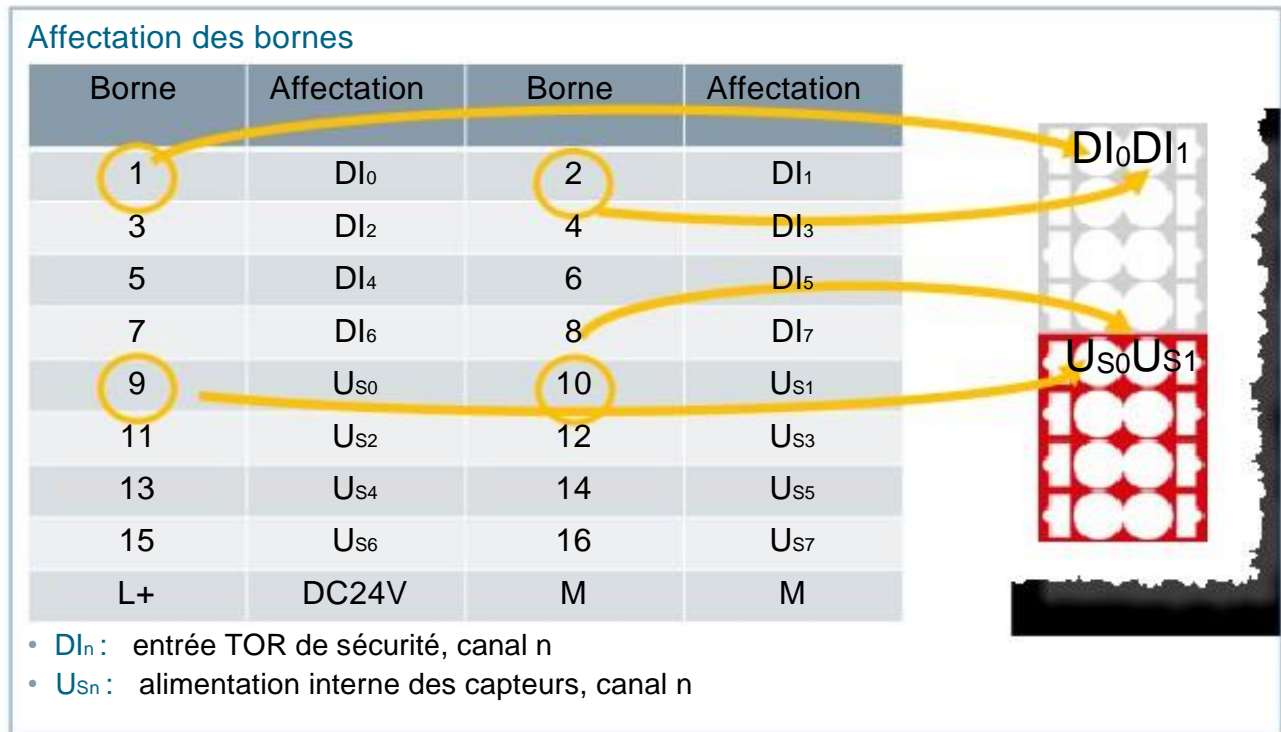
Résultat :

Tous les modules et la CPU devraient à présent être exempts d'erreurs.

5.18. Information complémentaire



5.18.1. Affectation des bornes ET200SP / F-DI



Affectation des bornes

Le module d'entrée TOR F-DI 8x24VDC HF possède 8 entrées de sécurité DI0 à DI7 (SIL3). Ces entrées peuvent être regroupées deux par deux en une seule entrée.

Vous pouvez regrouper les entrées suivantes :

- DI0 et DI4
- DI1 et DI5
- DI2 et DI6
- DI3 et DI7

Les signaux de process sont alors délivrés par les canaux DI0, DI1, DI2 et DI3.

Raccordement sur 2 canaux de deux capteurs à un canal (SIL3/Cat.3/PLe)

Pour chaque signal de process, deux capteurs à un canal (voir page 4-11, exemples à droite) qui acquièrent la même valeur de process sont raccordés à deux entrées du module F (évaluation 1oo2 (1de2)).

Raccordement sur 2 canaux d'un capteur à deux canaux (SIL3/Cat.4/PLe)

Pour chaque signal de process, un capteur à deux canaux est raccordé à deux entrées du module F (évaluation 1oo2 (1de2)). Alimenter les capteurs à partir de deux alimentations capteur différentes.

5.18.2. Affectation des bornes ET200SP / F-DQ

Affectation des bornes

Borne	Affectation	Borne	Affectation
1	DQ-P ₀	2	DQ-P ₁
3	DQ-P ₂	4	DQ-P ₃
5	DQ-P ₀	6	DQ-P ₁
7	DQ-P ₂	8	DQ-P ₃
9	DQ-M ₀	10	DQ-M ₁
11	DQ-M ₂	12	DQ-M ₃
13	DQ-M ₀	14	DQ-M ₁
15	DQ-M ₂	16	DQ-M ₃
L+	DC24V	M	M

- DQ-P_n : sortie TOR de sécurité, canal n, commutation P
- DQ-M_n : masse pour sortie TOR de sécurité, canal n, commutation M

Activation intempestive des modules périphériques avec sorties de sécurité

Si un module périphérique F avec sorties de sécurité risque d'être passivé pendant une période plus longue que celle indiquée dans les caractéristiques de sécurité (> 100 heures) sans que l'erreur soit corrigée, il faut interdire toute possibilité d'activation intempestive du module périphérique F par une seconde erreur qui ferait passer le système F à un état dangereux. Bien que la probabilité d'apparition de telles erreurs matérielles soit très faible, il convient d'éviter l'activation intempestive des modules périphériques F avec sorties de sécurité à l'aide de mesures techniques ou organisationnelles. L'une des possibilités est la coupure de l'alimentation en courant du module périphérique F passivé pendant une période de 100 heures, par exemple. Pour les installations disposant de normes produites, les mesures nécessaires sont normalisées.

Pour toutes les autres installations, l'exploitant doit mettre en place son propre concept de mesures et les faire valider par un expert.

Propriété de coupure de modules F avec sorties de sécurité

Une coupure spécifique au canal est réalisée en cas de détection d'une erreur. Il est également possible de réagir de manière échelonnée dans le temps à des états critiques du processus ou de couper les sorties de manière individuelle et sécurisée.

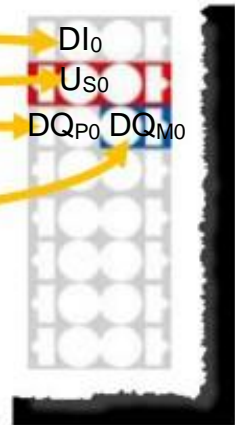
Connexion de charges non flottantes

Le F-DQ 4x24VDC/2A PM HF peut connecter des charges formant une liaison entre la masse et la terre d'au moins 100 kΩ. Sinon, un court-circuit est détecté. Du point de vue du module F, l'interrupteur M est shunté par la liaison masse-terre.

5.18.3. Affectation des bornes ET200SP / F-PM

Affectation des bornes

Borne	Affectation	Borne	Affectation
1	DI ₀	2	DI ₁
3	U _{S0}	4	U _{S1}
5	DQ-P ₀	6	DQ-M ₀
7	AUX	8	AUX
L+	DC24V	M	M
L+	DC24V	M	M



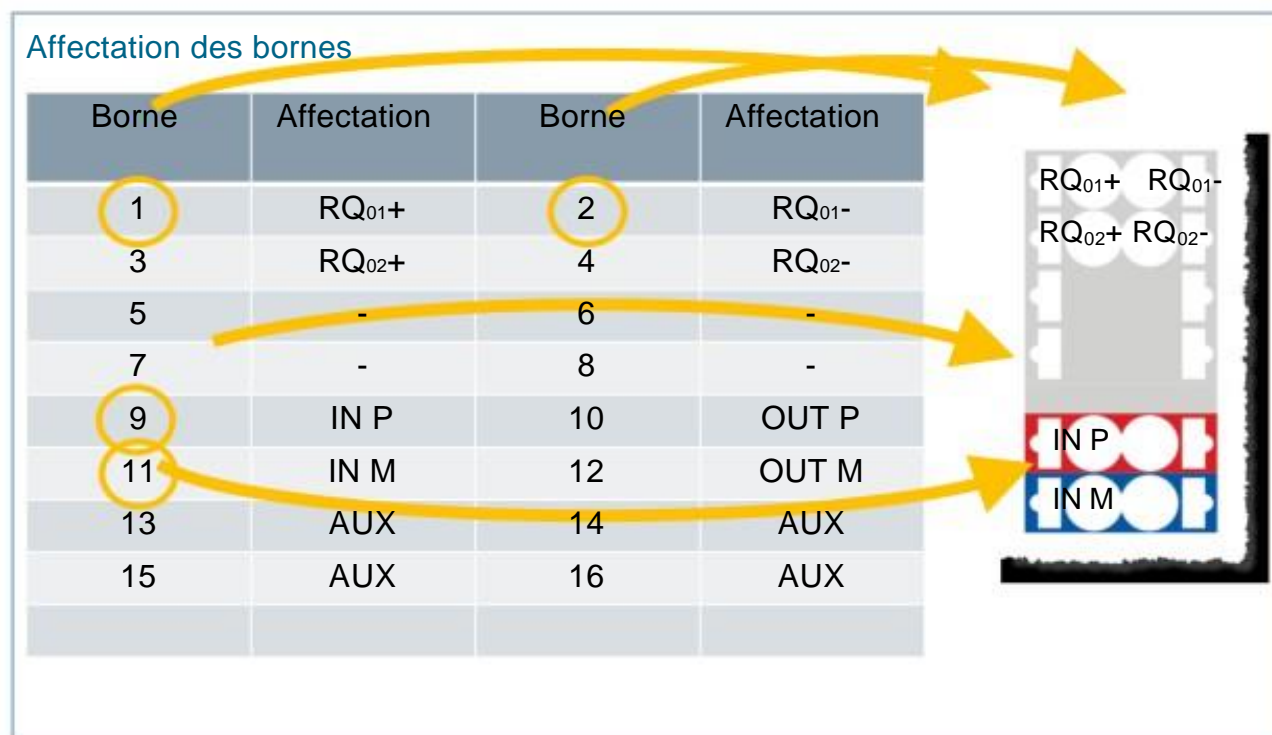
- **DI_n** : entrée TOR de sécurité, canal n
- **U_{Sn}** : alimentation interne des capteurs, canal n
- **DQ-P₀** : sortie TOR de sécurité, canal 0, commutation P
- **DQ-M₀** : masse pour sortie TOR de sécurité, canal 0, commutation M
- **AUX** : borne pour PE ou barre de potentiel (utilisable jusqu'à 230 V AC)

Affectation des entrées

Le module de puissance F-PM-E dispose de 2 entrées de sécurité DI0 et DI1 (SIL3). Les deux entrées peuvent être réunies en une seule.

Le canal DI0 délivre alors le signal de process. Les connexions des entrées sont équivalentes au module F-DI.

5.18.4. Affectation des bornes ET200SP / F-RQ



Raccordement de la tension de charge et de la charge

Les raccordements de sorties relais sont des contacts à fermeture libres de potentiel. Cela signifie que la tension d'alimentation doit être externe. Branchez l'alimentation de charge (alimentation 1) et la charge (charge 1) en série aux raccordements RQ01 (bornes 1;2). Les contacts à fermeture du relais assurent ainsi la coupure du courant d'alimentation de charge. Grâce aux deux contacts relais branchés en série, il est possible de poursuivre la mise hors circuit si l'un des deux relais est défectueux.

Le deuxième circuit est indépendant du premier sur le plan électrique. Ils sont logiquement reliés ensemble par la commande commune. Cela signifie qu'un autre potentiel peut régner dans le circuit à partir de RQ02 (bornes 3,4), de l'alimentation 2 et de la charge 2.

5.19. Catégories d'arrêt selon EN 60204-1

L'arrêt d'un entraînement peut être réalisé de plusieurs manières selon EN 60204-1 > 3 catégories d'arrêt :

Catégorie d'arrêt 0 (STO)

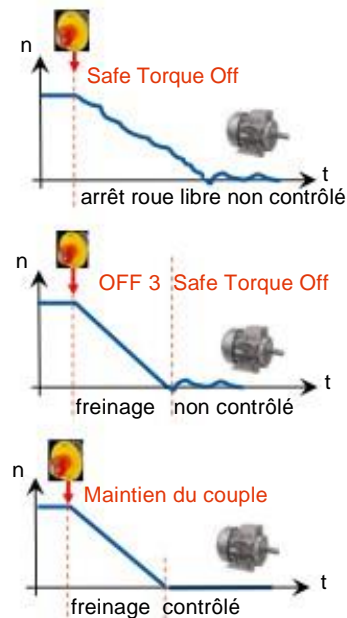
- Suppression immédiate de la puissance
- Coupure électromécanique ou électronique
- Séparation électrique non exigée

Catégorie d'arrêt 1 (SS1)

- Entraînement freiné électriquement jusqu'à l'arrêt
- Coupure de la puissance quand l'arrêt est obtenu
- Coupure électromécanique ou électronique
- Séparation électrique non exigée

Catégorie d'arrêt 2 (SS2)

- Entraînement freiné électriquement jusqu'à l'arrêt
- Maintien de la puissance à l'arrêt



EN 60204-1

Sécurité des machines ± Équipement électrique des machines ± Partie 1 : règles générales

Catégorie d'arrêt 0

Arrêt par suppression immédiate de la puissance sur les actionneurs ; ne doit pas être réalisé nécessairement avec des composants électromécaniques ; une séparation électrique n'est pas impérative.

Catégorie d'arrêt 1

Arrêt contrôlé en maintenant la puissance sur les actionneurs pour obtenir l'arrêt de la machine ; la puissance est ensuite coupée quand l'arrêt est obtenu

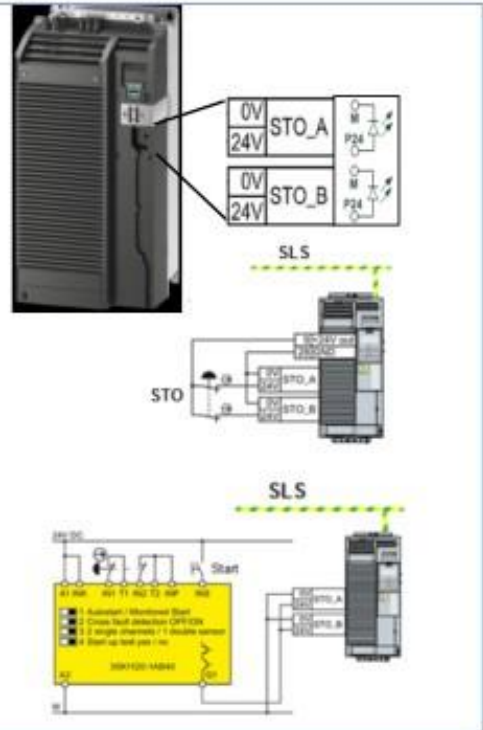
Arrêt contrôlé : arrêt du mouvement d'une machine en maintenant la puissance sur les actionneurs durant la procédure d'arrêt.

Catégorie d'arrêt 2

Arrêt contrôlé en maintenant la puissance sur les actionneurs

5.20. SINAMICS G120 : STO / SS1 en PL(e) SIL3 Arrêt d'urgence via bornes sur le PM240-2 FSD-FSF

- Sur le module de puissance SINAMICS PM240-2 FSD-F, la fonction STO est commandée via des bornes.
- La fonction STO est intégrée dans les Basic Functions de la CU240E-2 et de la CU250S-2.
- La fonction STO via bornes sur le PM240-2 FSD-FSF peut être utilisée en parallèle avec les fonctions Safety de la Control Unit.
- Le PM240-2 filtre les changements de signaux via des tests d'activation et de désactivation sur les entrées de sécurité (un filtre matériel supprime les changements de signaux ≤ 4 ms).
- La fonction répond au niveau de performance PL e selon EN ISO 13849-1:2006 ainsi qu'au niveau d'intégrité de sécurité SIL 3 selon CEI 61508:2010.
- Il est possible d'utiliser comme temps de réaction dans le cas le plus défavorable avec un variateur sans défaut 20 ms pour STO et 24 ms pour SBC.
- [Certificat](#)



5.21. Aides à la mise en œuvre de la technique de sécurité

	Contenu	Disponibilité
Safety Evaluation Tool	Outil d'évaluation du niveau de sécurité requis	Outil en ligne www.siemens.com/safety-evaluation-tool
Exemples de fonctions	Indications relatives aux fonctions et applications	Téléchargement sur Internet http://support.automation.siemens.com/WW/view/de/20208582/136000
Sitrain	Formations aux produits et aux normes	Contact Internet http://www.sitrain-learning.siemens.com/FR/fr/rw24924/Normes
Assistance	Une assistance adaptée à chaque phase du projet	Contact Internet http://support.automation.siemens.com

Table des matières

6.	Programmation	6-4
6.1.	Programme utilisateur d'une CPU F	6-5
6.2.	Blocs logiques du programme de sécurité	6-6
6.3.	Types de données et opérations	6-7
6.4.	Structure et traitement du programme de sécurité	6-8
6.4.1.	Bloc Main-Safety	6-9
6.4.2.	Groupe F-Runtime	6-10
6.5.	Le programme de sécurité	6-11
6.5.1.	Structure du programme de sécurité	6-12
6.5.2.	Séquence d'appel dans le programme de sécurité	6-13
6.5.3.	Créer un FC-F /FB-F	6-14
6.5.4.	Opérations logiques et fonctions safety dépendantes du mode de fonctionnement	6-15
6.5.5.	Connexion des données globales	6-16
6.5.6.	Bibliothèque de sécurité	6-17
6.5.7.	Multi Instance	6-18
6.5.8.	Constantes booléennes FALSE pour « 0 » et TRUE pour « 1 »	6-19
6.5.9.	Standardisation des blocs	6-20
6.6.	Editeur Safety Administration	6-21
6.6.1.	General	6-22
6.6.2.	Groupe F-Runtime	6-25
6.6.3.	Créer un groupe F-Runtime	6-26
6.6.4.	Groupe F-Runtime - Paramètres	6-27
6.6.5.	Blocs F	6-28
6.6.6.	Type de données API F adapté	6-29
6.6.7.	Protection d'accès	6-30
6.6.8.	Web Server F-Admins	6-31
6.6.9.	Paramètres (1)	6-32
6.6.10.	Paramètres (2)	6-34
6.6.11.	Flexible F-Link	6-35
6.7.	Protection du savoir-faire	6-36
6.7.1.	Mise en place	6-36
6.7.2.	Suppression	6-37
6.8.	Compilation	6-38
6.8.1.	Compiler le programme de sécurité (1)	6-38
6.8.2.	Compiler le programme de sécurité (2)	6-39
6.9.	Charger dans la CPU	6-40
6.9.1.	Charger le programme de sécurité dans la CPU (1)	6-40
6.9.2.	Charger le programme de sécurité dans la CPU (2)	6-41
6.9.3.	Charger le programme de sécurité dans la CPU (3)	6-42
6.10.	Charger sur PG/PC	6-43
6.10.1.	Charger le programme de sécurité sur PG/PC	6-43
6.11.	Tester le programme de sécurité	6-44
6.12.	Comparer des programmes de sécurité	6-45

6.13.	Bloc de données : RTG1SysInfo.....	6-46
6.14.	Spécificités du programme de sécurité (1)	6-47
6.15.	Spécificités du programme de sécurité (2)	6-48
6.16.	Echange des données entre le programme standard et le programme de sécurité	6-49
6.17.	Accès à la mémoire image.....	6-50
6.18.	Accès aux blocs de données	6-51
6.19.	Recommandation pour l'échange de données entre programme utilisateur standard et programme de sécurité	6-52
6.20.	Réinitialisation de la commande opérationnelle	6-53
6.21.	Contrôle de plausibilité.....	6-54
6.22.	Exercice 1: Configurer le Touchpanel.....	6-55
6.22.1.	Exercice 1 : Copier le projet Touchpanel, le DB Interface et les FC de la bibliothèque	6-56
6.22.2.	Exercice 1 : Adapter la connexion de l'IHM	6-57
6.22.3.	Exercice 1 : Adapter l'adresse IP et le nom d'appareil PROFINET	6-58
6.22.4.	Exercice 1 : Synchroniser les variables IHM et API et compiler.....	6-59
6.22.5.	Exercice 1 : Chargement de l'IHM et de la CPU.....	6-60
6.22.6.	Exercice 1 : Assurer l'échange de données cohérent entre IHM et CPU	6-61
6.23.	Affichage « Mode de sécurité désactivé »	6-62
6.23.1.	Exercice 2 : Effacer un groupe d'exécution existant.....	6-63
6.23.2.	Exercice 2 : Création manuelle d'un nouveau groupe d'exécution.....	6-64
6.23.3.	Exercice 2 : Création du Pre-processing d'un groupe d'exécution.....	6-65
6.23.4.	Exercice 2 : transfert de données vers le programme de sécurité	6-66
6.23.5.	Exercice 2 : définition des groupes de blocs et du « Main_Safety »	6-67
6.24.	Passivation des modules F	6-69
6.24.1.	Principe	6-69
6.24.2.	Blocs de données de la périphérie de sécurité.....	6-70
6.24.3.	Variables des DB de périphérie	6-71
6.24.4.	État de la valeur des CPU 1200/1500F.....	6-73
6.24.5.	Bits d'état de la valeur pour F-DI	6-74
6.24.6.	Bits d'état de la valeur pour F-DQ	6-75
6.24.7.	Bits d'état de la valeur pour F-PM	6-76
6.24.8.	Bits d'état de la valeur pour F-AI	6-77
6.25.	Exercice 3 : Comprendre l'état de la valeur	6-78
6.26.	Exercice 4 : Réintégration de la périphérie F.....	6-79
6.27.	Exercice 5 : Evaluation de l'état de la périphérie F.....	6-80
6.28.	Exercice 6 : Encore un test pour comprendre l'état de la valeur	6-82
6.28.1.	Exercice 6 : Test du câblage des entrées et sorties de sécurité	6-83
6.29.	Exercice 7 : programmer les modes de fonctionnement	6-84
6.29.1.	Exercice 7 : Organigramme	6-85
6.30.	Exercice 8: Dispositif de levage	6-86
6.30.1.	Exercice 8: Organigramme	6-87
6.30.2.	Exercice 8 : Diagnostic dans le programme safety.....	6-88
6.30.3.	Fonction de sécurité ESTOP1	6-90
6.31.	Exercice 9 : Etiqueteuse	6-91
6.31.1.	Exercice 9: Organigramme	6-92
6.31.2.	La fonction de sécurité : TWO_H_EN.....	6-94
6.31.3.	La fonction de sécurité : FDBACK	6-95
6.32.	Exercice 10: Transport.....	6-96
6.32.1.	Exercice 10 : Organigramme	6-97
6.32.2.	La fonction de sécurité : SFDOOR	6-99

6.33.	Exercice 11 : Poste de contrôle	6-100
6.33.1.	Exercice 11 : Organigramme	6-101
6.34.	Aperçu des exercices complémentaires	6-102
6.34.1.	Exercice complémentaire 1 : Visualisation des informations du groupe d'exécution	6-103
6.34.2.	Exercice complémentaire 2 : Acquittance globale de la périphérie de sécurité	6-104
6.34.3.	Exercice supplémentaire 3 : acquittance de sécurité avec l'IHM	6-106
6.35.	Informations complémentaires	6-109
6.35.1.	Liens.....	6-110
6.35.2.	Structure et traitement du programme de sécurité (300F/400F)	6-111
6.35.3.	Groupe séquentiel (300F/400F)	6-112
6.35.4.	F_GLOBDB (300F/400F)	6-113
6.35.5.	Variables du DB de périphérie (300F/400F)	6-114
6.35.6.	DB de périphérie de sécurité / Différences lors de l'évaluation (1).....	6-115
6.35.7.	DB de périphérie de sécurité / Différences lors de l'évaluation (2).....	6-116

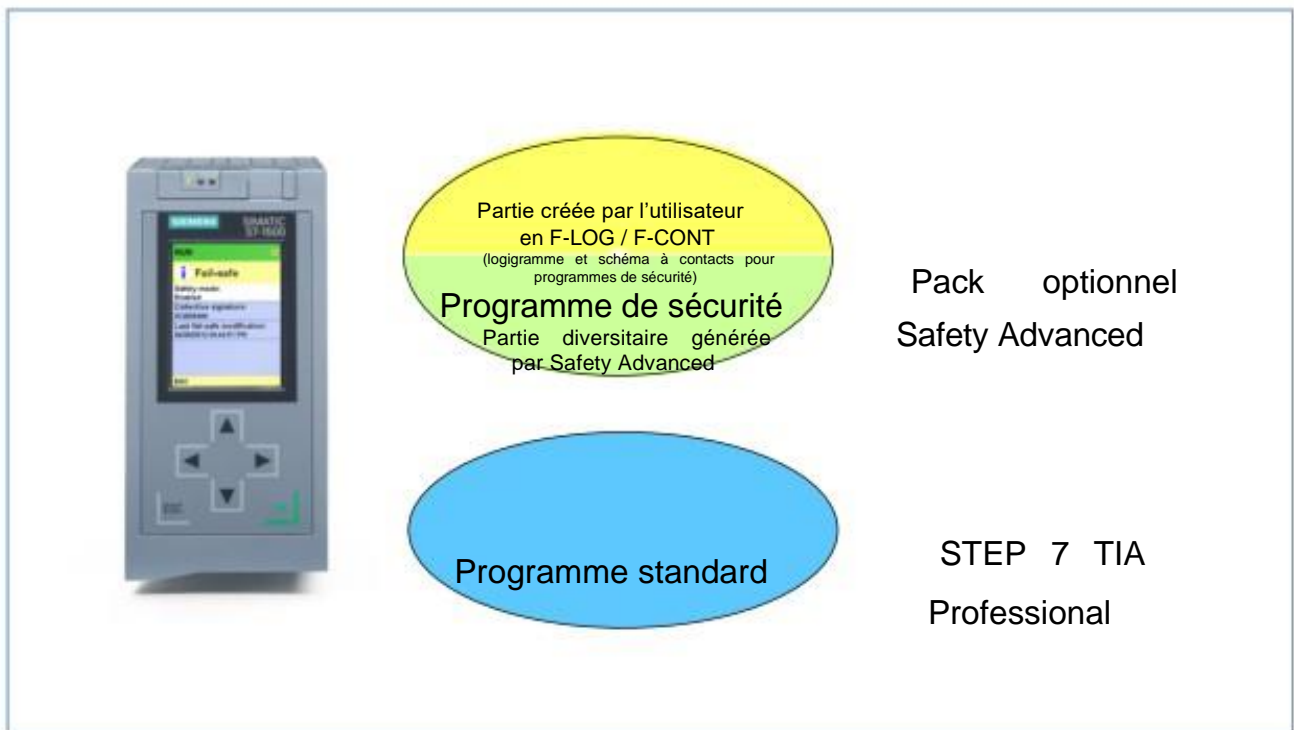
6. Programmation

→ l'issue de la formation, le participant au stage

- ... saura expliquer la structure d'un programme destiné à une application de sécurité (programme de sécurité ou programme F)
- ... saura expliquer quelles fonctions sont programmées dans le programme standard et dans le programme de sécurité
- ... saura expliquer et programmer un échange de données entre le programme standard et le programme de sécurité
- ... connaîtra et saura utiliser les opérations autorisées dans le programme de sécurité
- ... connaîtra et saura utiliser les fonctions de sécurité indiquées
- ... saura programmer la dépassivation des modules de sécurité



6.1. Programme utilisateur d'une CPU F



Programme utilisateur d'une CPU de sécurité

Le programme utilisateur d'une CPU de sécurité (CPU F - Failsafe) se compose d'un programme standard pour la commande des fonctions standard et d'un programme de sécurité additionnel pour la commande des fonctions de sécurité (application de sécurité).

Le programme standard est créé comme précédemment par l'utilisateur à l'aide du STEP 7 standard, le programme de sécurité à l'aide du pack STEP 7 « Safety Advanced ».

La programmation s'effectue dans l'éditeur CONT/LOG standard de STEP 7. Des fonctions de sécurité CEI certifiées peuvent également être intégrées dans le programme.

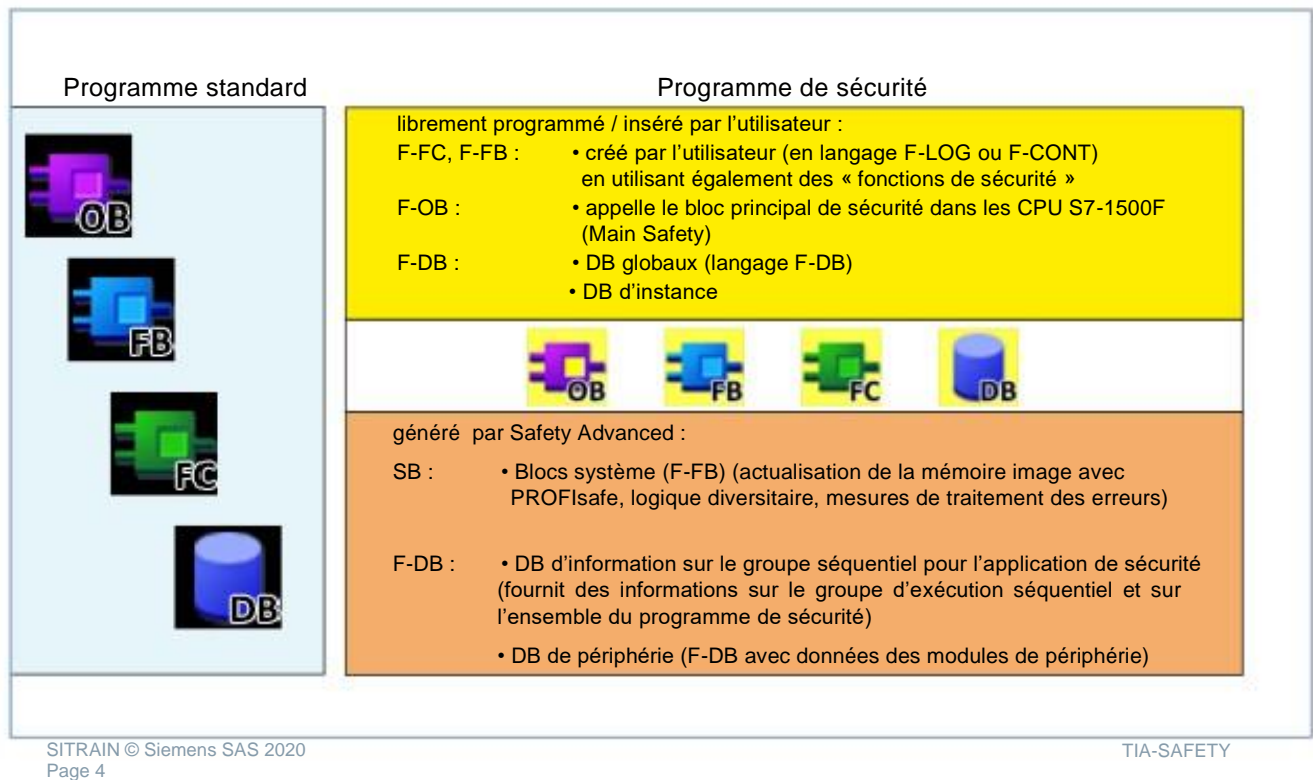
Programme de sécurité

Le programme de sécurité (programme F) se compose d'une partie créée par l'utilisateur en LOG ou CONT et d'une partie générée par Safety Advanced contenant notamment la logique de diversité par rapport à la partie utilisateur.

Coexistence programme standard / programme de sécurité

Le programme standard et le programme de sécurité sont traités indépendamment l'un de l'autre par la CPU. En raison de la coexistence des deux programmes sur une même CPU, la communication entre eux peut être assurée à l'aide de variables globales. Les modifications du programme standard n'ont aucune incidence sur le programme de sécurité, de sorte que son intégrité soit toujours garantie.

6.2. Blocs logiques du programme de sécurité



Les fonctions de sécurité requises sont librement programmables par l'utilisateur en « F-LOG » (logigramme pour programmes de sécurité) et/ou « F-CONT » (schéma à contacts pour programmes de sécurité). Ces langages de programmation correspondent pour l'essentiel aux langages LOG/CONT standard, avec toutefois certaines restrictions (jeu d'opérations, types de données et plages d'opérandes admissibles).

F-DB

Le programme de sécurité comporte également des blocs de données pour la mémorisation des données globales. Les blocs de données de sécurité (F-DB) sont créés/modifiés/utilisés comme les DB standard. Seuls les types de données utilisables sont limités par rapport aux DB standard. Les blocs de données d'instance des FB de sécurité (qu'ils aient été créés par l'utilisateur ou copiés à partir de fonctions de sécurité de Safety Advanced) ne sont pas édités par l'utilisateur comme dans le programme standard, mais générés par STEP 7.

SB

Pour créer un programme de sécurité exécutable à partir du programme de sécurité programmé par l'utilisateur, Safety Advanced génère des blocs système de sécurité (SB) sous forme de F-FB lors de l'enregistrement et de la compilation de la configuration matérielle ainsi que lors de la compilation du programme de sécurité. Ces blocs permettent de détecter les erreurs / les défauts, et d'assurer une réaction adéquate afin d'amener le système de sécurité à un état sûr en cas de défaillance. Ils réalisent en outre la communication entre la CPU F (mémoire image) et la périphérie de sécurité via le protocole de sécurité PROFIsafe.

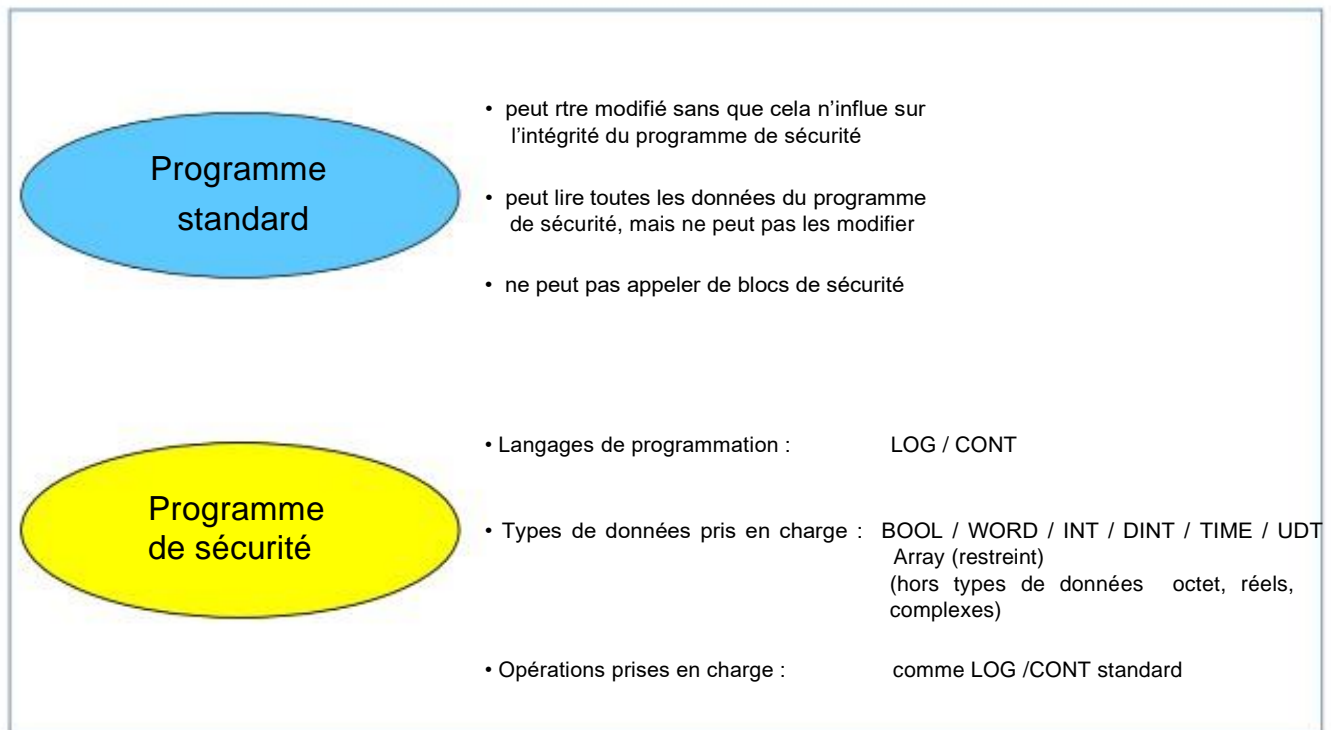
DB d'information sur le groupe d'exécution

Le DB d'information sur le groupe d'exécution de la séquence de programme de sécurité (groupe séquentiel) met à disposition des informations pour la séquence de programme de sécurité exécutée et pour l'ensemble du programme de sécurité.

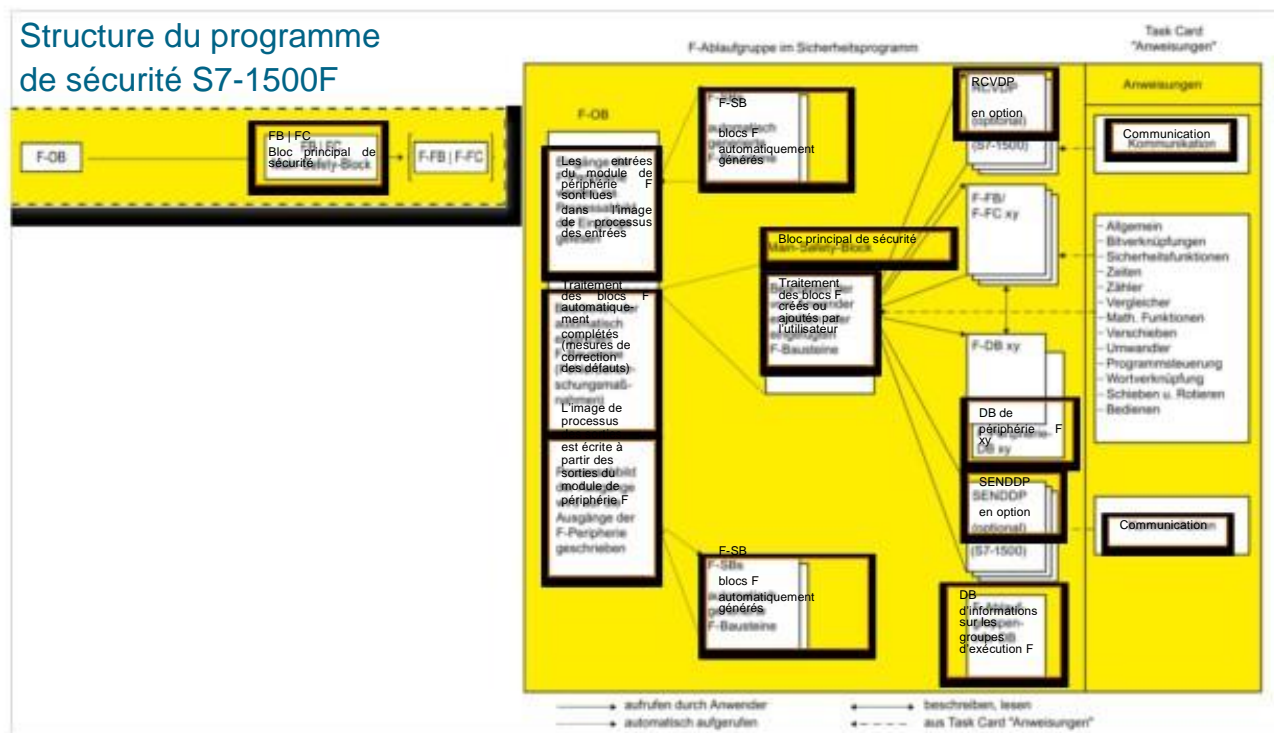
F-OB

F-OB appelle le bloc main safety d'un groupe d'exécution F dans une CPU S7-1500 F.

6.3. Types de données et opérations



6.4. Structure et traitement du programme de sécurité



Structure du programme de sécurité, groupes d'exécution d'une séquence de programme de sécurité

Tout comme le programme standard, le programme de sécurité peut être programmé de manière structurée. Le programme de sécurité peut se composer d'un ou deux groupes séquentiels indépendants l'un de l'autre qui constituent des programmes autonomes. Ces groupes séquentiels assurent l'exécution d'une séquence du programme de sécurité. La subdivision en deux groupes séquentiels permet de distinguer, au sein du programme de sécurité, les fonctions de sécurité critiques en terme de temps de celles qui ne sont pas critiques. Plus le temps de réaction d'une fonction de sécurité doit être court dans un processus, plus l'intervalle d'appel du groupe séquentiel qui contient la fonction de sécurité (ou du F-OB dans lequel le bloc principal de sécurité est programmé) doit être bref.

L'intégration d'un groupe séquentiel ou du bloc principal de sécurité correspondant dans un F-OB garantit que le programme de sécurité sera exécuté dans des intervalles de temps définis, ce qui est indispensable à la détermination des temps de réaction du programme de sécurité et des fonctions de sécurité de l'installation.

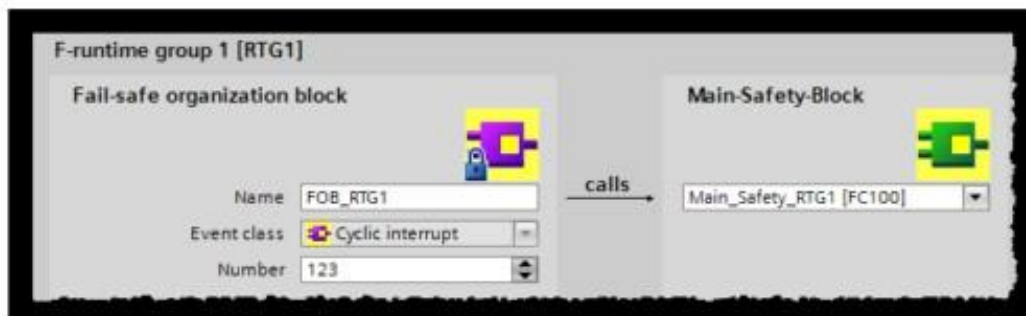
Instructions destinées au programme de sécurité

Vous trouverez dans l'onglet « Instructions », en fonction de la CPU F utilisée, des instructions utilisables pour la programmation du programme de sécurité. Vous retrouverez des instructions déjà connues que vous utilisez pour la programmation du programme utilisateur standard, comme des opérations sur bits, des fonctions mathématiques, des fonctions de gestion du programme et des opérations sur mots. Celles-ci sont complétées par des instructions de sécurité destinées, par exemple, à la surveillance de commandes bimanuelles, l'analyse de discordance, l'inhibition, l'arrêt/coupure d'urgence, la surveillance de porte de protection, la surveillance de boucle de retour, et par des instructions destinées à la communication de sécurité entre CPU F.

6.4.1. Bloc Main-Safety

Bloc Main Safety

- Premier bloc F qui peut être programmé par l'utilisateur
- Appelle tous les blocs F créés par l'utilisateur et spécifiques à l'application
- Doit être assigné à un groupe d'exécution F (Safety Administration)
- Paramétrage par défaut TIA Portal: un groupe d'exécution comprenant le bloc Main-Safety est généré automatiquement avec l'appel dans le F-OB lors de la création d'une CPU-F

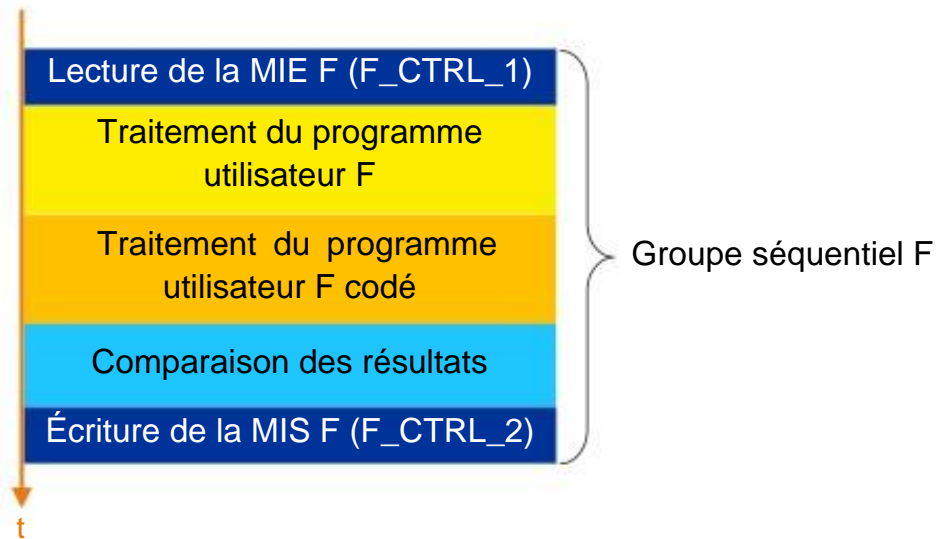


Bloc Main Safety (Bloc principal de sécurité)

Chaque groupe séquentiel (groupe F-runtime) est représenté par un « bloc principal de sécurité », qu'il s'agisse d'une fonction ou d'un bloc fonctionnel (F-FC ou F-FB), qui permet d'accéder au programme de sécurité et dont l'appel est généralement programmé dans un bloc d'organisation (F-OB). L'utilisateur peut directement programmer la logique du programme de sécurité dans ce bloc et/ou utiliser ce dernier pour structurer le programme de sécurité et appeler d'autres blocs de sécurité. Parallèlement au programme créé par l'utilisateur dans le bloc principal de sécurité, Safety Advanced lance d'autres appels de blocs générés automatiquement avec lesquels sont réalisées les fonctions de sécurité servant de pilotes pour les modules de périphérie, ou contenant la logique de diversité, etc.

6.4.2. Groupe F-Runtime

Groupe séquentiel de sécurité en détail (avec ordre du traitement) :



2 groupes séquentiels de sécurité maximum par CPU F

Groupes d'exécution d'une séquence de programme de sécurité (F-runtime groups)

Pour assurer davantage de maniabilité, un programme de sécurité se compose d'un ou de deux groupes séquentiels (F-runtime group). Un groupe séquentiel est une structure logique comprenant plusieurs blocs de sécurité combinés au sein d'un même système de sécurité (groupe d'exécution d'une séquence de programme de sécurité).

Un groupe séquentiel se compose :

- d'un bloc d'organisation (F-OB) qui appelle le bloc principal de sécurité
- d'un bloc principal de sécurité (F-FB/F-FC que vous affectez au F-OB)
- le cas échéant, d'autres F-FB/F-FC que vous programmez avec LOG/CONT et que vous appelez à partir du bloc principal de sécurité
- le cas échéant, d'un ou plusieurs F-DB
- des DB de périphérie de sécurité
- d'un DB d'information sur le groupe séquentiel
- des blocs de sécurité issus de la bibliothèque du projet ou de bibliothèques globales
- des blocs système F-SB
- de blocs de sécurité automatiquement générés (blocs du compilateur).

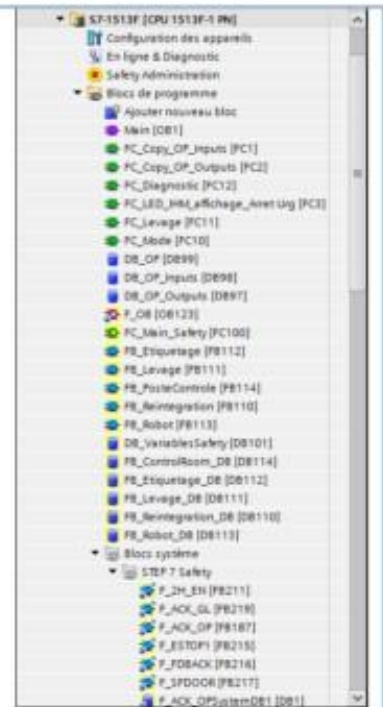
Structure du programme de sécurité avec deux groupes séquentiels

Vous pouvez diviser votre programme de sécurité en deux groupes séquentiels. Si vous exécutez des séquences du programme de sécurité à un niveau d'exécution plus rapide, vous obtenez des boucles de sécurité plus rapides avec des temps de réaction plus courts.

6.5. Le programme de sécurité

Le programme de sécurité contient toujours«

- des blocs F créés par l'utilisateur
 - Gestion dans le dossier Blocs de programme
 - Appel à partir du bloc principal de sécurité
- des blocs F générés par le système (Coded Processing)
 - Créés lors de la compilation du programme utilisateur
 - Gestion par le système dans des dossiers Blocs propres
 - Complètent le programme utilisateur avec
 - des mesures de traitement des erreurs
 - des vérifications liées à la sécurité



Remarque

Vous ne devez pas insérer des blocs système F du dossier « Blocs système » dans un bloc principal de sécurité Main Safety FB-F/FC-F.

6.5.1. Structure du programme de sécurité

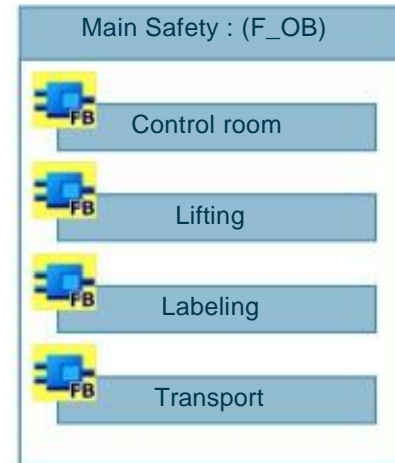
Définir la structure du programme

- Diviser le programme en modules, par ex.
 - Pour la détection, l'évaluation et le pilotage –
- Ou en fonction des unités de production
- Créer au préalable une spécification pour chaque module (basée sur l'analyse de risques).
- Eviter les équations de traitement complexes.

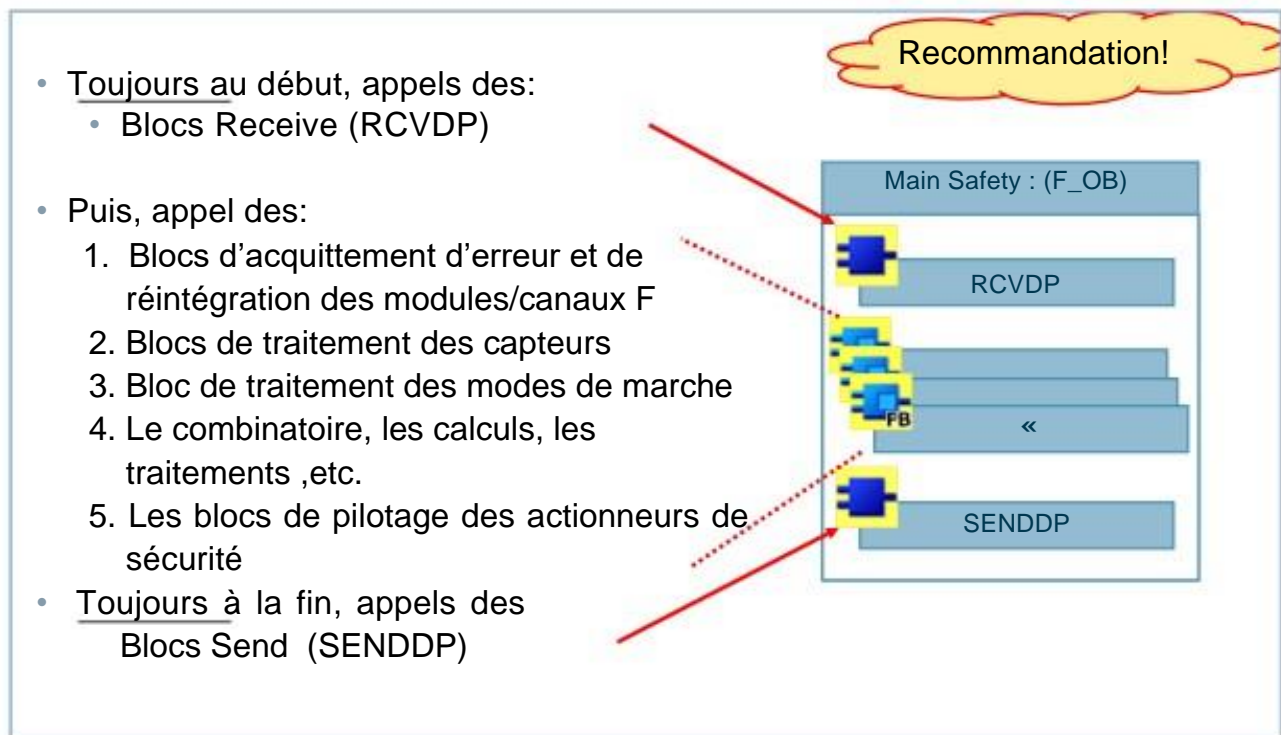
Bénéfices

- Complexité réduite.
- Réduction des erreurs de programmation.
- Extension simplifiée et simplification de réception avec les fonctions réutilisées.
- Réutilisation de parties de programme sans réception.
- Les éléments du programme déjà codés sont testés et réceptionnés au préalable.

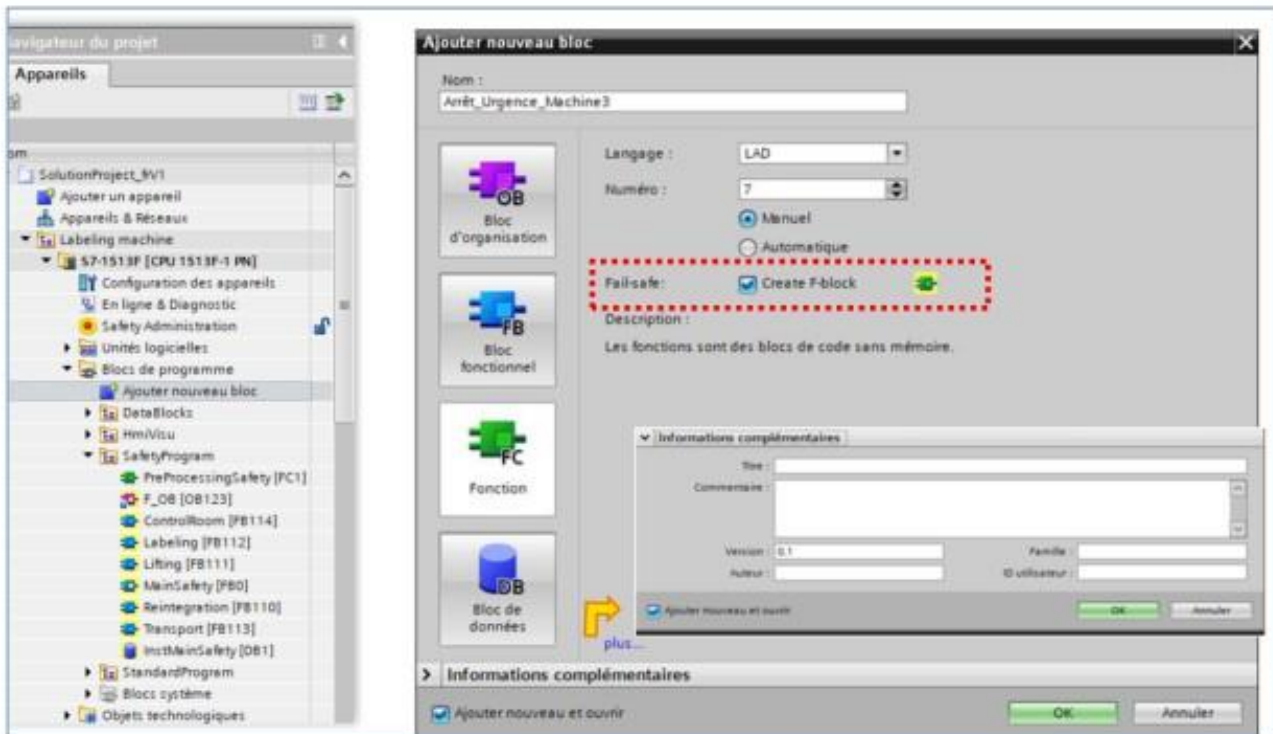
Recommandation!



6.5.2. Séquence d'appel dans le programme de sécurité



6.5.3. Créer un FC-F /FB-F



F-FC / F-FB

Les fonctions (FC) ou les blocs de fonction (FB) du programme de sécurité sont créés de la même manière que ceux du programme standard ; il suffit d'activer l'option « Fail-safe » ou « Create F-block ».

Bloc principal de sécurité (Main Safety block)

Le bloc principal de sécurité d'un groupe séquentiel est créé et programmé de la même manière que n'importe quel autre bloc de sécurité. L'utilisateur peut directement programmer la logique de sécurité dans ce bloc et/ou utiliser ce dernier pour structurer le programme de sécurité et appeler d'autres blocs de sécurité.

La propriété selon laquelle un F-FC ou un F-FB doit faire office de bloc principal de sécurité n'est attribuée à ce bloc que lors de la création du groupe séquentiel dans Safety Administration. Lors de la compilation du programme de sécurité, les appels de blocs générés par Safety Advanced sont regroupés dans le bloc principal de sécurité.

6.5.4. Opérations logiques et fonctions safety dépendantes du mode de fonctionnement

Programmation des opérations logiques

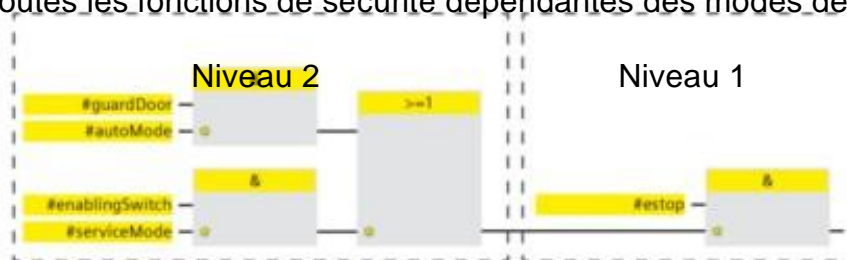
- Utiliser de préférence les éléments logiques ET et OU
- Réduire l'utilisation des blocs SR au strict minimum
- Eviter les sauts pour la logique binaire

Recommandation!

Programmation des fonctions de sécurité dépendantes du mode de fonctionnement

Diviser la logique en deux niveaux différents (voir IEC 62061):

- Niveau 1: toutes les fonctions de sécurité indépendantes des modes de marche ou des états de l'installation.
- Niveau 2: toutes les fonctions de sécurité dépendantes des modes de marche.

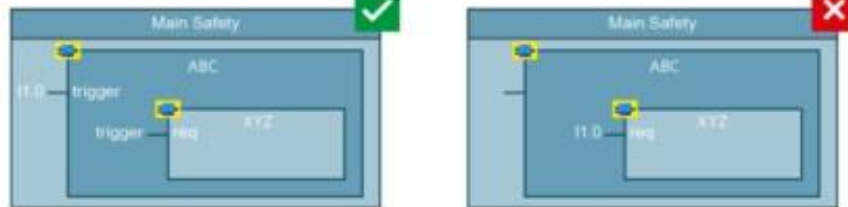


6.5.5. Connexion des données globales

Connexion

- Connecter les données globales (entrées, sorties, blocs de données) au niveau le plus élevé de la hiérarchie des blocs (Main Safety)
- Utiliser les interfaces du bloc pour transmettre les signaux aux niveaux inférieurs

Recommandation!



Avantages

- Concept de blocs modulaires
- Des parties de programmes peuvent être réutilisées dans d'autres projets sans adaptations → signature identique
- Les erreurs de programmation sont réduites.
- Le programme complet est plus lisible car la fonction générale d'un bloc peut déjà être évaluée à partir de ses interfaces.

6.5.6. Bibliothèque de sécurité

Fonctions de sécurité de la bibliothèque

- Contient des blocs de sécurité certifiés pour les fonctions de sécurité suivantes :

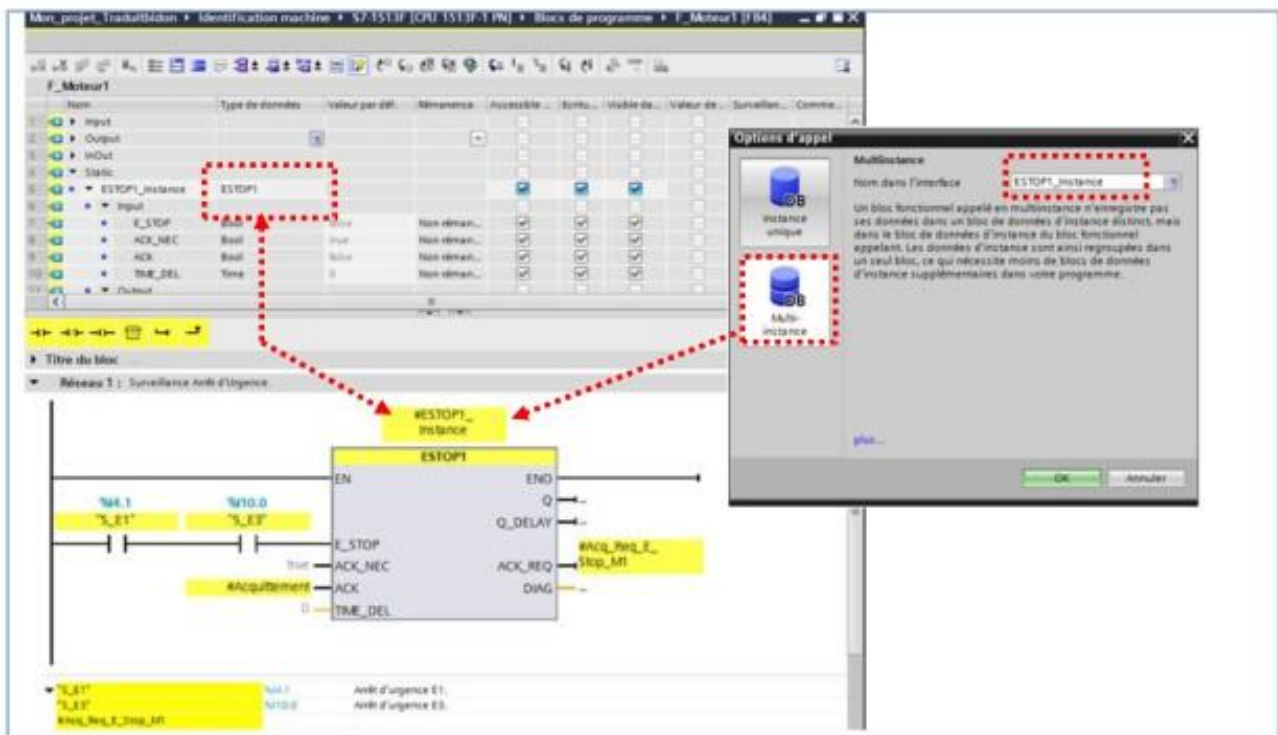
Instructions de base		
Nom	Description	Version
General		
Bit logic operations		
Safety functions		V1.8
ESTOP1	Emergency STOPemer...	V1.6
TWO_H_EN	Two-hand monitoring ...	V1.3
MUT_P	Parallel muting	V1.4
EV1oo2DI	1oo2 evaluation with d...	V1.3
FDBACK	Feedback monitoring	V1.5
SFDOOR	Safety door monitoring	V1.3
ACK_GL	Global acknowledgme...	V1.3
Timer operations		V1.7
Counter operations		V1.7
Comparator operations		
Math functions		
Move operations		V2.0
Conversion operations		V2.0
Program control operati...		
Word logic operations		
Shift and rotate		V2.0
Operate		V1.7
ACK_OP	Fail-safe acknowledgm...	V1.3

Communication		
Nom	Description	Version
PROFIBUS / PROFINET		V2.0
SENDP	Send data (16 BOOL, 2...	V2.0
RCVDP	Receive data (16 BOOL...	V2.0
Failsafe HMI Mobile Panels		V3.0

Instructions pour le programme de sécurité

Vous trouverez dans l'onglet « Instructions », en fonction de la CPU F utilisée, des instructions utilisables pour la programmation du programme de sécurité. Vous retrouverez des instructions déjà connues que vous utilisez pour la programmation du programme utilisateur standard, comme des opérations sur bits, des fonctions mathématiques, des fonctions de gestion du programme et des opérations sur mots. Celles-ci sont complétées par des instructions de sécurité destinées, par exemple, à la surveillance de commandes bimanuelles, l'analyse de discordance, l'inhibition, l'arrêt/coupure d'urgence, la surveillance de porte de protection et la surveillance de boucle de retour.

6.5.7. Multi Instance



Multi Instance

STEP 7 exploite le concept de la multi-instance dans les programmes de sécurité afin de permettre le style de programmation orienté objet. Cela permet de déclarer et d'appeler des instances multiples pour des fonctions utilisateur tout comme pour des fonctions safety.

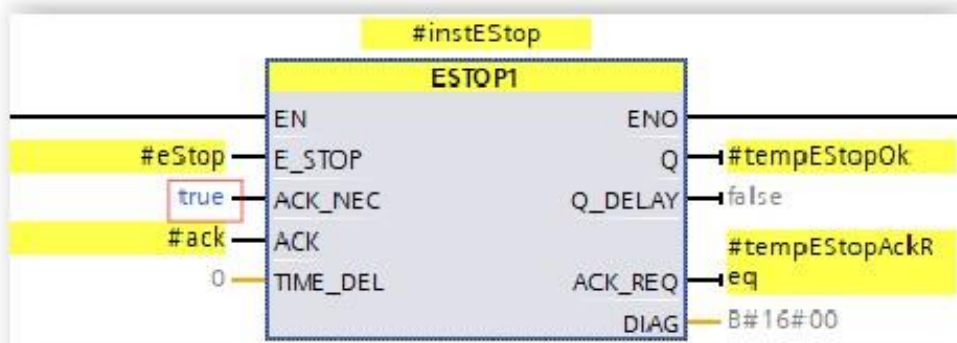
Blocs de sécurité

La programmation des appels de blocs de sécurité s'effectue de la même façon que celle des blocs standard. Par principe, seuls les appels de blocs de sécurité sont autorisés dans le programme de sécurité. Le système ne propose donc que des blocs de sécurité dans les dossiers « Blocs FB » et « Blocs FC » de l'éditeur. Lors de l'intégration ou de la programmation de l'appel d'une fonction de sécurité, les DB d'instance nécessaires sont générés par STEP 7.

6.5.8. Constantes booléennes FALSE pour « 0 » et TRUE pour « 1 »

Programmation avec TRUE et FALSE

Pour les CPU F du S7/1200 et S7-1500, vous disposez des constantes booléennes « FALSE » pour « 0 » et « TRUE » pour « 1 » en tant que paramètres effectifs pour l'affectation des paramètres formels lors de l'appel des blocs. Une connexion aux opérations booléennes est également possible.



6.5.9. Standardisation des blocs

Standardisation

Créer des blocs modulaires et réutilisables:

- Blocs pour des capteurs de sécurité typiques
- Blocs pour des actionneurs de sécurité typiques
- Blocs pour des fonctions fréquemment utilisées (par ex. réintégration, mode de marche)

Recommandation!

Avantages

- Les blocs réutilisés ne nécessitent plus de validation
- Programmation plus efficace des fonctions et projets ultérieurs
- Gestion des versions avec le concept de bibliothèque du TIA Portal
- Standardisation des paramètres formels pour les projets et les programmeurs pour une lisibilité et des tests optimisés

Information complémentaire

- [Introduction to standardization \(DI-STAND\)](#)

La standardisation présente les avantages suivant pour l'utilisateur

- Le logiciel devient plus transparent pour l'utilisateur et donc plus facile à utiliser.
- Réduction significative des sources d'erreurs grâce à l'utilisation de parties de programme déjà validées.
- Minimisation de l'effort de création et de mise en service du programme lorsque le standard est disponible.
- Simplification des diagnostics et du dépannage.
- Documentation claire des modules avec un comportement défini.
- Pas d'ingénierie parallèle pour la même tâche.
- Interfaces définies avec d'autres services.

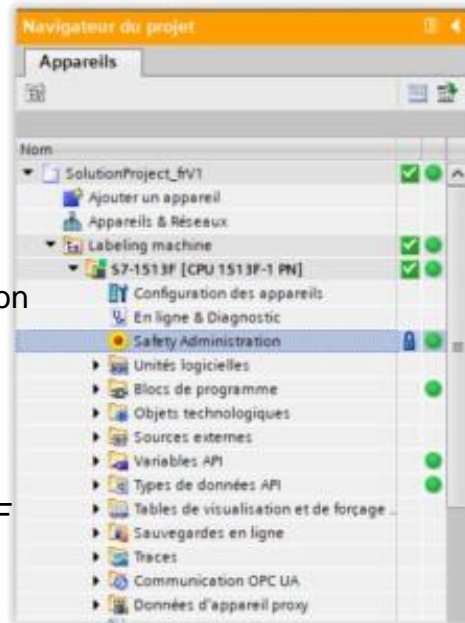
La standardisation présente les avantages suivants pour le fabricant.

- Les exigences des clients existants (par exemple, l'industrie automobile) sont satisfaites.
- Maintien et développement de la compétitivité.
- Augmentation de l'efficacité de l'ingénierie.
- Gestion simplifiée des versions de machines (flexibilité).
- Répartition des tâches par lots de travail.
- Réduction des coûts grâce à la mise en service virtuelle / « Digital Twin ».

6.6. Editeur Safety Administration

L'éditeur « Safety Administration » vous aide pour les tâches suivantes:

- Afficher l'état et le mode du programme de sécurité
- Afficher les signatures F
- Créer/organiser les groupes runtime F
- Informations pour les blocs F
- Informations pour les types de données API F
- Informations pour utilisateurs avec autorisation F-Admin
- Définir/modifier les protections d'accès
- Définir les réglages des paramètres du programme de sécurité
- Créer/visualiser/effacer les communications F via Flexible F-Link (S7-1200, S7-1500)



Général

→ cette rubrique s'affichent l'état du mode de sécurité, l'état du programme de sécurité et la signature globale F.

Groupes séquentiels (F-runtime groups)

Un programme de sécurité se compose d'un ou deux groupes d'exécution de séquences de programmes de sécurité (groupe séquentiel). Vous définissez dans cette rubrique les blocs et les propriétés du groupe d'exécution d'une séquence de programme de sécurité.

Blocs de sécurité (F-blocks)

Vous obtenez à cette rubrique des informations sur les blocs de sécurité utilisés dans votre programme de sécurité et leurs propriétés.

Types de données API adaptés aux applications de sécurité (F-compliant PLC data types)

Vous obtenez à cette rubrique des informations sur les types de données API adaptés aux applications de sécurité créés par l'utilisateur (UDT). Vous pouvez également vérifier si un type de données API adapté aux applications de sécurité (UDT) est utilisé dans le programme de sécurité.

Protection d'accès (Access protection)

Vous pouvez créer, modifier ou supprimer à cette rubrique le mot de passe du programme de sécurité. Une protection d'accès est obligatoire pour le mode production.

Administrateurs F serveur Web (Web server F-admins)

Vous obtenez à cette rubrique des informations sur les utilisateurs ayant l'attribut « F-Admin » pour le serveur Web de la CPU F.

Flexible F-Link

Sous « Flexible F-Link » vous obtenez des informations tabellaires au sujet des communications safety ainsi programmées.

6.6.1. General

- Sous « Général » s'affichent l'état du mode de sécurité, l'état du programme de sécurité et la signature globale du programme de sécurité.

La fonction « Désactiver le mode de sécurité » permet la commande de variables dans les CPU S7-1500F

Les signatures globales F identifient clairement une version du programme de sécurité et des paramètres de sécurité de la F-CPU et de la périphérie F. Elles sont importantes pour la réception sur site du programme de sécurité.

État du mode de sécurité (Safety mode status)

Affiche l'état courant du mode de sécurité. Condition préalable : une liaison en ligne doit être établie avec la CPU F sélectionnée.

Désactiver le mode de sécurité (Disable safety mode)

Lorsqu'une liaison en ligne est établie et le mode de sécurité activé, vous pouvez désactiver ici le mode de sécurité de la CPU F sélectionnée à l'aide du bouton « Désactiver le mode sécurité ». Le mode de sécurité ne peut être désactivé que pour l'ensemble du programme de sécurité (et non pour des groupes d'exécution F individuels). Condition préalable : la case « Le mode de sécurité peut être désactivé » doit être activée sous « Paramètres ».

État du programme de sécurité (Safety program status)

Affiche l'état courant de votre programme en ligne et hors ligne.

- Cohérent (avec information si aucun mot de passe n'a été affecté)
- Non cohérent

Signature du programme (Program signature)

Sous « Program signature » différentes signature s'affiche. Chaque signature provient de différentes parties des données sécuritaires du projet.

- Collective F-signature : cette signature est modifiée lors de chaque modification des données sécuritaires du projet. Elle englobe les signatures suivantes.
- Software F-signature (S7-1200/1500) : cette signature est modifiée lors de modifications du programme de sécurité.
- HW F-signature (S7-1200/1500) : cette signature est modifiée par modifications au niveau de la configuration matérielle sécuritaire.
 - F-communications-Adresse-signature (S7-1200/1500) : cette signature est modifiée par modification du nom ou de l'identifiant UUID des liaisons de communication F-Link.

6.6.1.1. Signature fonctionnelle

La signature fonctionnelle facilite la comparaison et la validation de votre programme de sécurité. Elle est uniquement modifiée lorsqu'une modification relative à la sécurité est réalisé dans le projet:

Effet sur la signature:

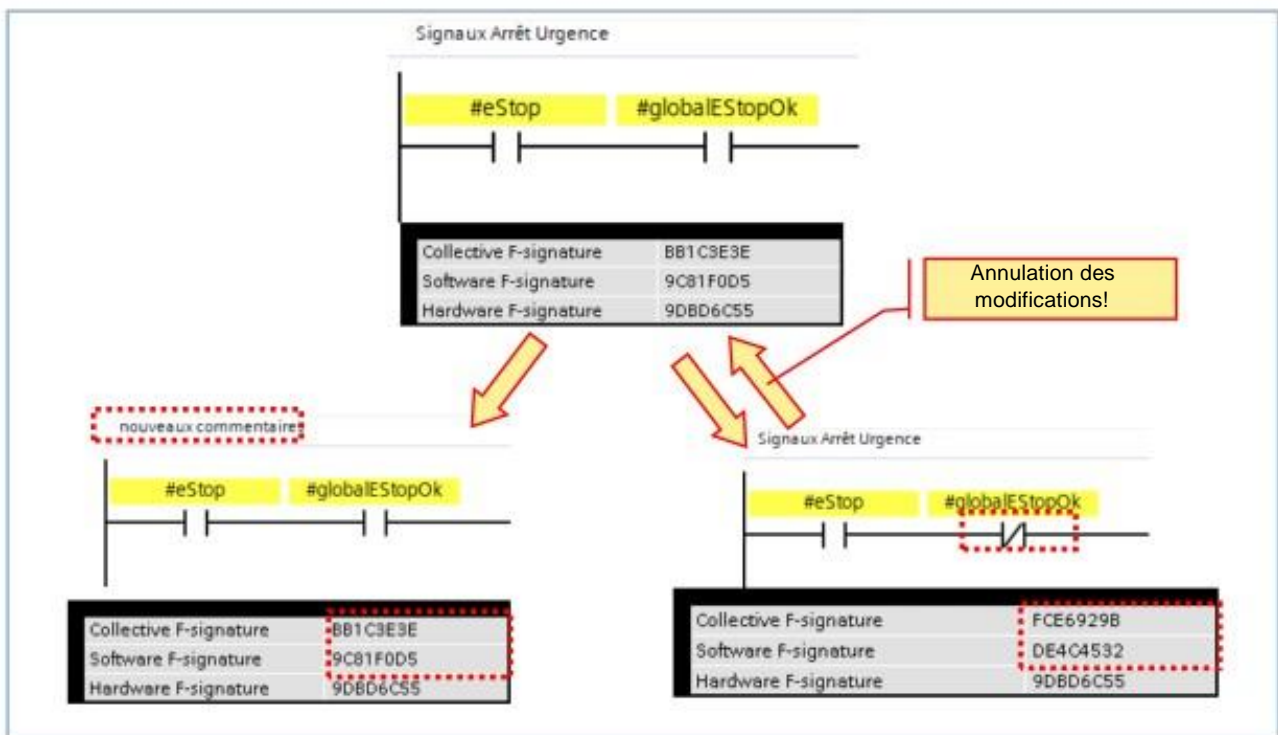
- Logique des blocs F
- Ordre d'appel des blocs F
- Paramètres F de la CPU et de l'ensemble des E/S de sécurité
- Paramètres des groupes d'exécution F

Aucun effet sur la signature:

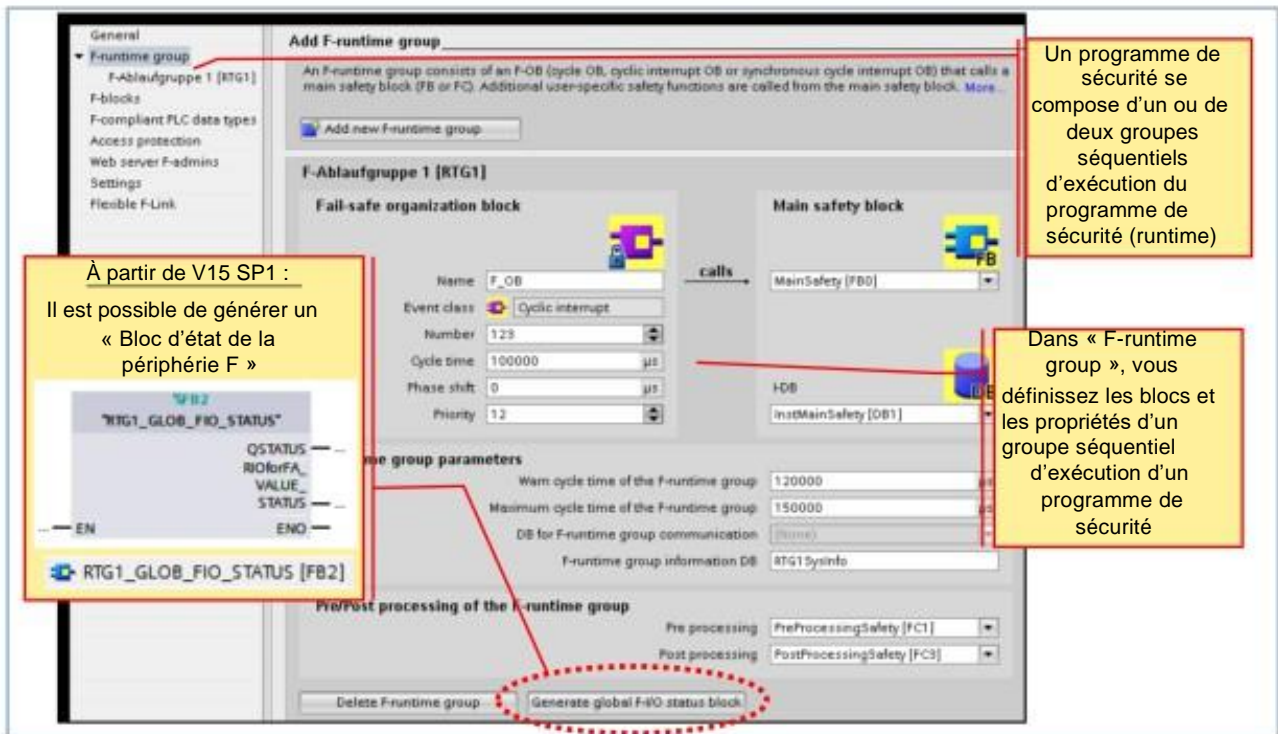
- Commentaires
- Symbolique
- Horodatage

IMPORTANT:
L'annulation des modifications restaure également la « vieille » signature.

6.6.1.2. Exemple de signature fonctionnelle



6.6.2. Groupes F-Runtime



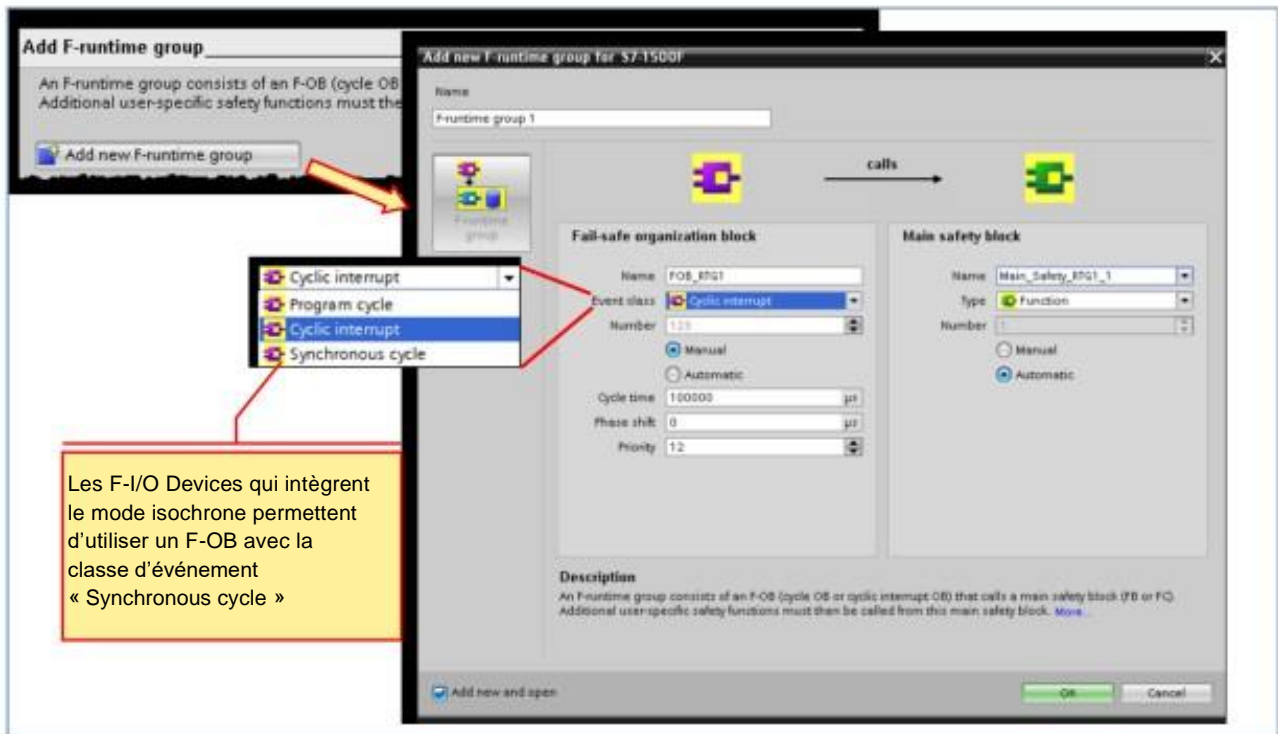
Règles à respecter :

- L'accès aux canaux (valeurs de canaux et états des valeurs) d'une périphérie de sécurité n'est autorisé qu'à partir d'un seul groupe d'exécution.
- L'accès à des variables du DB d'une périphérie de sécurité n'est autorisé qu'à partir d'un groupe séquentiel, à savoir celui depuis lequel l'accès aux canaux ou à l'état des valeurs de cette périphérie de sécurité est réalisé (si l'accès est réalisé).
- Les F-FB peuvent être utilisés dans plusieurs groupes séquentiels, mais ils doivent être appelés avec des DB d'instance distincts.
- L'accès aux DB d'instance est autorisé uniquement à partir du groupe séquentiel dans lequel le F-FB correspondant est appelé.
- L'accès aux variables d'un F-DB global n'est autorisé qu'à partir d'un groupe séquentiel (un F-DB global peut cependant être utilisé dans plusieurs groupes séquentiels).
- (S7-1200, S7-1500) Vous ne pouvez pas appeler vous-même le bloc principal de sécurité (Main Safety). Il est automatiquement appelé par le F-OB correspondant.
- (S7-1200, S7-1500) Le F-OB doit être créé avec le plus haut niveau de priorité de tous les OB.
- La mémoire image des entrées et sorties de la périphérie standard, les mémentos et les variables des DB du programme utilisateur standard sont accessibles en lecture comme en écriture à partir de plusieurs groupes d'exécution F (voir également « Échanges de données entre le programme utilisateur standard et le programme de sécurité »).

Générer un bloc d'état global de la périphérie F

Vous pouvez créer un bloc standard (FB) portant le nom « RTGx_GLOB_FIO_STATUS », qui indiquera si pour un module de périphérie F ou au moins un canal des valeurs de remplacement sont activées au lieu des valeurs du processus. Le résultat de l'interrogation est reporté à la sortie « QSTATUS ». Les périphéries F qui ont été désactivées avec la variable « DISABLE » du DB de périphérie ne sont pas concernées. La sortie « RIOforFA_VALUE_STATUS » correspond à la sortie « QSTATUS » mais uniquement pour la périphérie F avec profil « RIOforFA-Safety ».

6.6.3. Créer un groupe F-Runtime



Pour le F-OB vous pouvez opter pour « Program cycle », « Cyclic interrupt » ou « Synchronous cycle ».

Par défaut le F-OB est de type « Cyclic interrupt ». Pour modifier la classe d'évènement du F-OB d'un groupe d'exécution F déjà activé, il faut effacer et recréer ce groupe d'exécution F.

Interruption cyclique

Nous préconisons un F-OB avec pour classe d'évènement « Cyclic interrupt » pour l'OB alarme cyclique. Ainsi le programme de sécurité est appelé à intervalles réguliers.

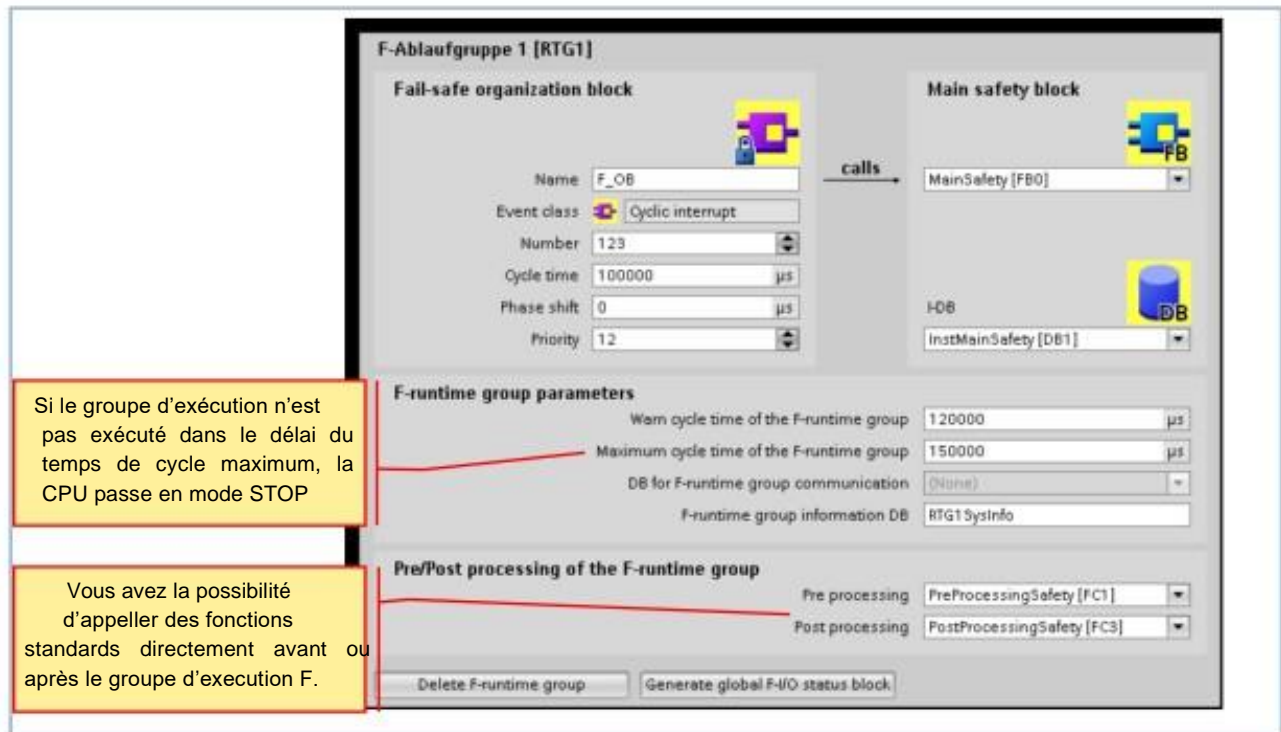
Cycle programme

F-OBs avec la classe d'évènement « Program cycle » ne sont pas recommandés car ils ont la plus faible priorité « 1 ».

Cycle synchrone

F-OBs avec la classe d'évènement « Synchronous cycle » sont uniquement adaptés à la périphérie F supportant l'isochronisme, par ex. « Télégramme Profisafe 902 » du SINAMICS S120 CU310-2 PN V5.1.

6.6.4. Groupe F-Runtime - Paramètres



Paramètres du groupe d'exécution d'une séquence de programme de sécurité (F-runtime group)

La CPU F effectue une surveillance du temps de cycle F dans le groupe d'exécution F. Vous disposez à cet effet de deux paramètres :

- En cas de dépassement de la limite d'avertissement du temps de cycle (« Warn cycle time of the F-runtime group »), une entrée est créée dans la mémoire tampon de la CPU F. Vous pouvez utiliser ce paramètre pour déterminer, par exemple, si le temps de cycle dépasse une valeur requise sans que la CPU F passe à l'état STOP.
- En cas de dépassement du temps de cycle maximal du groupe d'exécution séquentiel (« Maximum cycle time of the F-runtime group »), la CPU F passe à l'état STOP. Choisissez comme temps de cycle maximal du groupe séquentiel, le temps maximal qui peut s'écouler entre deux appels de ce groupe séquentiel (maximum 20 000 000 µs).

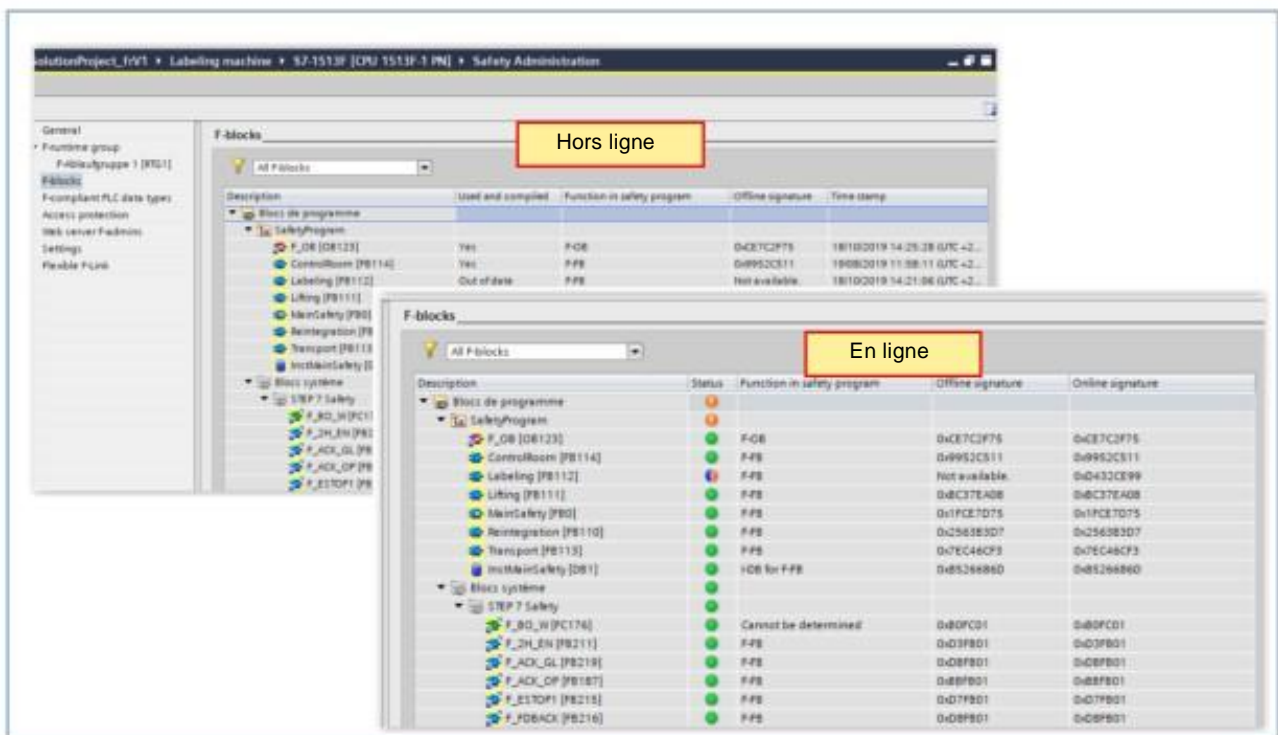
Entrez dans le champ DB d'information « F-runtime group information DB » un nom pour le DB d'information pour le groupe d'exécution du programme de sécurité.

Pré-/post- traitement

Avec le pré et posttraitement vous avez la possibilité d'appeler des blocs standards (FCs) immédiatement avant ou après un groupe d'exécution F, par ex. pour le transfert des données de communication sécuritaire via Flexible F-Link.

- Uniquement utilisable pour des FC standards.
- Les données locales temporaires et les constantes sont uniquement exploitables dans l'interface d'un FC Standard.
- Le temps de traitement du groupe d'exécution se prolonge du temps d'exécution des FC standard pour le pré-/post traitement (modifie TRTG_CURR et TRTG_LONG du DB d'information du groupe d'exécution F : RTG1Sysinfo).
- Comme le pré-/ post traitement ne modifie pas la fonctionnalité du programme de sécurité, la signature globale de sécurité reste identique après la compilation.

6.6.5. Blocs F



Informations affichées

Les informations suivantes sur les blocs de sécurité s'affichent en mode hors ligne :

- Le bloc de sécurité a-t-il été compilé et utilisé ?
- Fonction du bloc sécurité dans le programme de sécurité
- Signature hors ligne
- Horodatage de la dernière modification

Les informations suivantes sur les blocs de sécurité s'affichent en mode en ligne :

- État (si le bloc a le même horodatage en ligne et hors ligne)
- Fonction du bloc de sécurité dans le programme de sécurité
- Signature hors ligne
- Signature en ligne
- Les blocs de sécurité s'affichent par ordre hiérarchique comme dans le dossier « Blocs de programme ».

Fonction filtre

La fonction filtre permet de choisir entre une visualisation de tous les blocs de sécurité d'un groupe d'exécution donné ou de tous les blocs de sécurité du programme de sécurité.

- Sélectionnez « All F-blocks » dans la liste déroulante pour voir tous les blocs de sécurité.
- Sélectionnez un groupe séquentiel dans la liste déroulante pour voir tous les blocs de sécurité de ce groupe d'exécution.

6.6.6. Type de données API F adapté

- Les F-UDT (types de données API adaptés) se déclarent et s'utilisent exactement comme les UDT.
- Tous les types de données autorisés dans le programme de sécurité peuvent être utilisés dans les F-UDT.
- Les F-UDT ne peuvent pas être imbriqués à d'autres F-UDT.
- Les F-UDT peuvent être aussi bien utilisés dans le programme de sécurité que dans le programme standard.



Informations affichées

Les informations suivantes sur les types de données API adaptés (UDT) s'affichent en mode hors ligne :

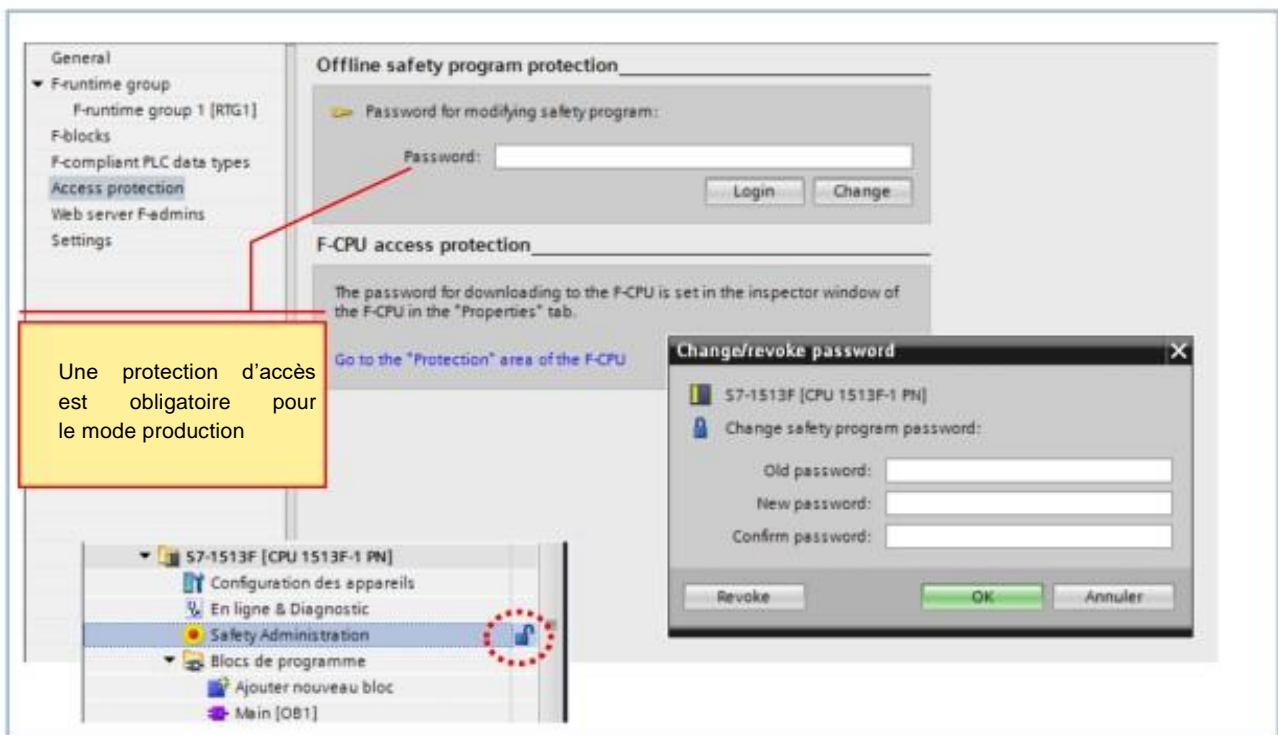
- Le type de donnée API adapté à un programme de sécurité est-il utilisé dans le programme de sécurité ?
- Horodatage de la dernière modification

Les informations suivantes sur les types de données API adaptés (UDT) s'affichent en mode en ligne :

- État (si les types de données API adaptés (UDT) ont les mêmes horodatages en ligne et hors ligne)

Les types de données API adaptés (UDT) s'affichent par ordre hiérarchique comme dans le dossier « Types de données API ».

6.6.7. Protection d'accès



Vue d'ensemble de la protection d'accès

L'accès au système de sécurité SIMATIC Safety peut être protégé par deux mots de passe, à savoir le mot de passe du programme de sécurité et le mot de passe de la CPU F.

Pour le mot de passe du programme de sécurité, deux versions sont à distinguer :

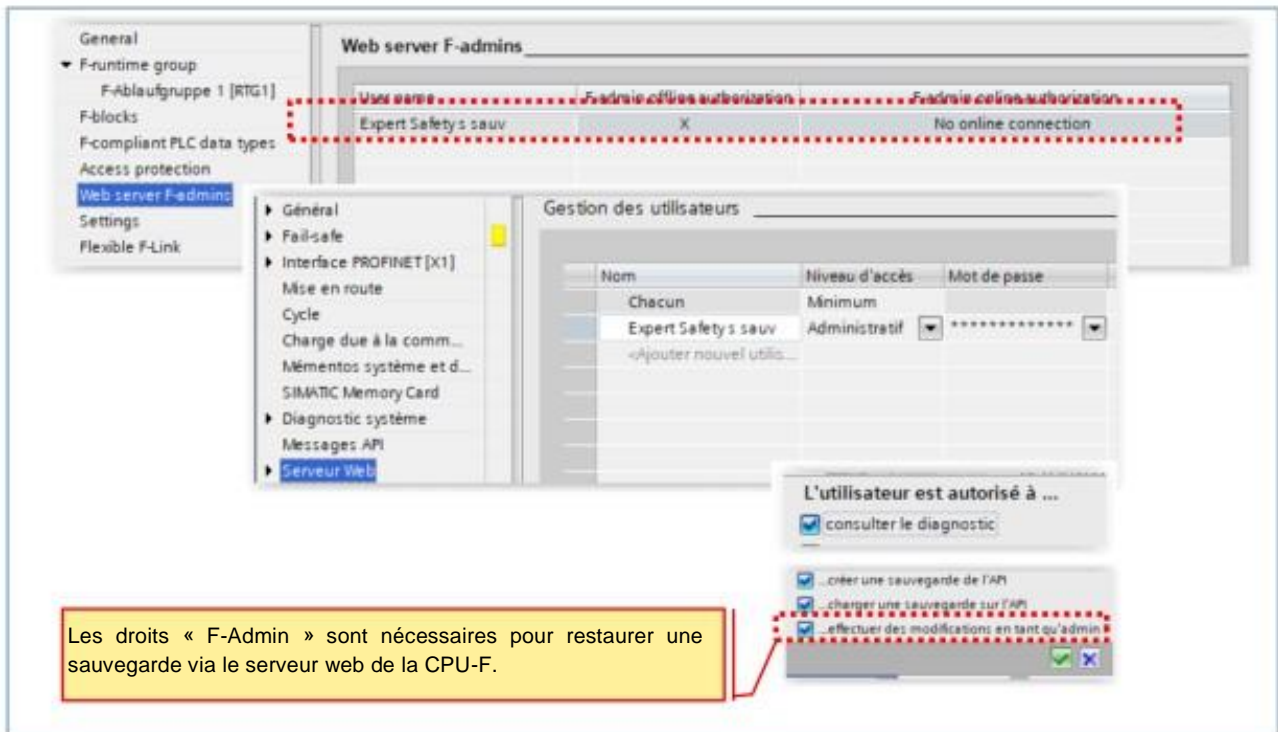
- Le mot de passe hors ligne, qui fait partie du programme de sécurité dans le projet hors ligne stocké dans la PG / le PC.
- Le mot de passe en ligne, qui fait partie du programme de sécurité stocké dans la CPU F.

Remarque :

Les modifications des DB standards auxquels le programme de sécurité accède en lecture ou en écriture exigent une nouvelle compilation du programme de sécurité. Ces DB standards ne sont pas soumis aux droits d'accès applicables au programme de sécurité.

Notez que vous avez également besoin du mot de passe en ligne pour charger les modifications de la configuration matérielle liées à la sécurité. Ceci vaut également pour les modifications de la périphérie de sécurité qui n'est pas utilisée dans le programme de sécurité. Pour garantir un chargement cohérent, vous devez également recompiler et recharger le programme de sécurité.

6.6.8. Web Server F-Admins

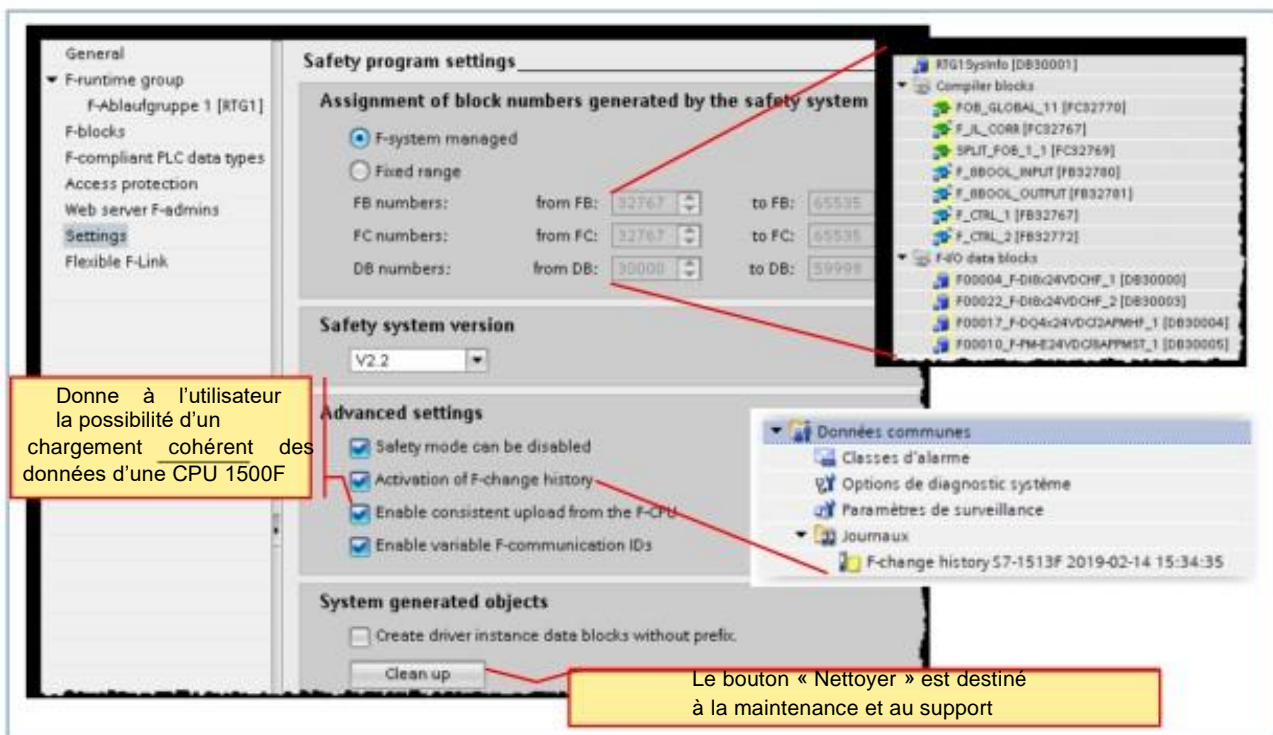


Fonctionnalité

Vous avez besoin du droit « F-Admin » pour restaurer une sauvegarde via le serveur Web de votre CPU F. Le droit « F-Admin » est attribué dans l'outil de configuration matérielle de la CPU F dans la « Gestion des utilisateurs » du serveur Web.

Cette fenêtre affiche des informations sur les utilisateurs possédant ce droit en ligne ou hors ligne pour les CPU F qui gèrent le droit « F-Admin ». Cela vous permet de savoir si une modification du droit « F-Admin » a un effet sur la CPU F. Pour rendre effective une modification du droit « F-Admin », vous devez charger la configuration dans la CPU F.

6.6.9. Paramètres (1)



Plages de numéros des blocs système de sécurité générés

Les séries de numéros paramétrés ici sont utilisées par le système de sécurité pour les nouveaux blocs de sécurité créés automatiquement.

- F-system managed : les séries de numéros sont automatiquement gérées par le système de sécurité en fonction de la CPU F utilisée. Le système de sécurité choisit une plage de numéros libre. Les plages de début et de fin des séries de numéros s'affichent.
- Fixed range : vous pouvez sélectionner vous-même les plages de début et de fin des séries de numéros dans la plage libre. La plage libre dépend de la CPU F utilisée.

Version du système de sécurité

Ce paramètre vous permet de définir la version du système Safety (notamment la version des blocs système et des blocs de sécurité automatiquement générés). Aucune modification de ce paramètre n'est normalement nécessaire. Lors de la création d'une nouvelle CPU F avec STEP 7 Safety, la version disponible la plus élevée est paramétrée par défaut.

Objets générés par le système

Le bouton « Nettoyer » (Clean up) est prévu pour la maintenance et le support.

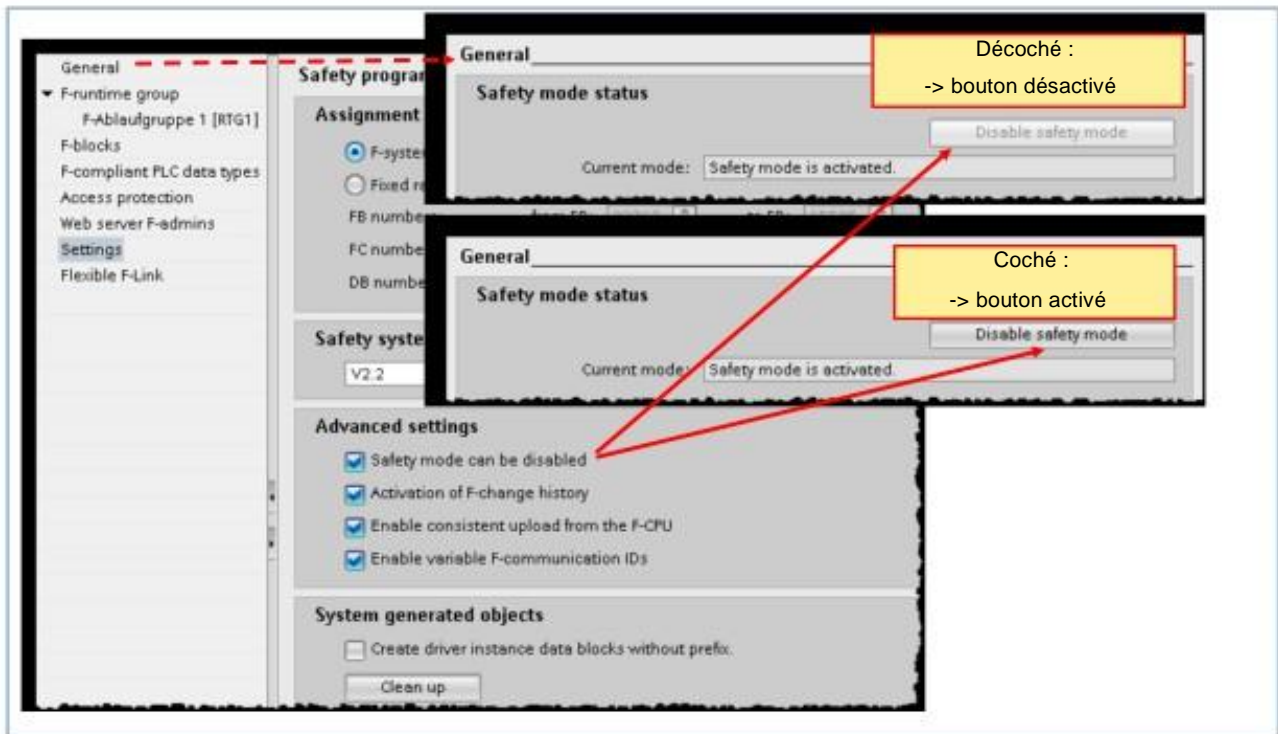
Permettre un chargement cohérent depuis la CPU F (Enable consistent upload from the F-CPU)

Cette option vous permet de charger sous forme cohérente à partir de la CPU F les données projet chargées (y compris des données projet de sécurité). Cette option n'est activable que si la CPU F et le microprogramme (firmware) de la CPU F gèrent le chargement des données projet (y compris les données projet de sécurité). Les CPU S7-1500F avec firmware à partir de V2.1 gèrent cette fonction, mais pas les contrôleurs logiciels S7-1500 F. À chaque modification de cette option, vous devez charger les données projet dans la CPU F. Notez que l'activation de cette option allonge le temps de chargement des données projet de sécurité dans la CPU F.

Activer des ID de communication F variables

Si vous activez cette option, vous pouvez affecter des valeurs variables à partir d'un DB-F global à l'entrée DP_DP_ID de l'instruction SENDP ou RCVDP.

6.6.10. Paramètres (2)



Le mode sécurité peut être désactivé

En désactivant l'option « Le mode sécurité peut être désactivé », vous évitez que le mode de sécurité d'un programme de sécurité puisse être désactivé.

Après une modification de cette option, vous devez recompiler le programme de sécurité et le recharger dans la CPU F pour que la modification prenne effet. Cela modifie la signature globale F de votre programme de sécurité.

Avant de passer au mode production et avant la réception du programme de sécurité, nous vous recommandons de désactiver cette option afin d'empêcher toute désactivation involontaire du mode de sécurité.

Activer l'historique des modifications F

L'option « Activer l'historique des modifications F » de l'éditeur Safety Administration vous permet d'activer la consignation des modifications du programme de sécurité dans un journal.

L'historique des modifications F se comporte comme l'historique des modifications standard.

Un historique des modifications F est créé pour chaque CPU F dans le Navigateur du projet sous « Données/historiques communs ».

Les éléments suivants sont enregistrés dans l'historique des modifications F :

- Signature globale F
- Nom de l'utilisateur
- Horodatage de la compilation
- Chargement du programme de sécurité avec horodatage
- Blocs de sécurité compilés avec signature et horodatage

L'historique des modifications F peut contenir au maximum 5 000 entrées par CPU F. Lorsque les 5 000 entrées sont dépassées, un nouvel historique des modifications est créé avec le schéma de nom suivant : « Historique modifications F <Nom CPU> AAAA-MM-JJ hh:mm:ss ».

6.6.11. Flexible F-Link

Flexible F-Link settings

Name	PLC Data Type	Direction	F-monitoring ti...	F-communicat
1 Envoi au partenaire	typeSafetyCommunication	Send	500	8a5f66ba-4c01-4e4d-863b-2319da4297bc
2 Reception depuis partenaire	typeSafetyCommunication	Receive	500	63c9e58a-643d-49d3-9607-57aaf72fab8e
3 <Add new>				

Possible à partir de la version V2.2 du système safety

F-communication UUID	Output data variable	Input data tag
8a5f66ba-4c01-4e4d-863b-2319da4297bc	"Envoi au partenaire".SEND_ARRAY[]	"Envoi au partenaire".ACK...
63c9e58a-643d-49d3-9607-57aaf72fab8e	"Reception depuis partenaire".SEND_ARRAY[]	"Reception depuis partena...

L' UUID de la communication safety assure l'unicité de l'ID de la communication de sécurité au delà des frontières du réseau.

Dans la zone « Flexible F-Link », vous créez de nouvelles F-communications, obtenez des informations sur les communications existantes et supprimez des communications.

Prérequis

- CPU-F S7-1500 avec Firmware V2.0 ou >
- CPU-F S7-1200 avec Firmware V4.2 ou >
- Version du système Safety V2.2 ou >

Information sur les communications F créés

Dans la zone « Flexible F-Link », vous recevez des informations sur les communications F configurées sous forme de tableau :

- Nom unique de la communication F au niveau de la CPU
- Type de données API (UDT) conforme pour envoyer et recevoir des données
- Direction de la communication F : Envoi/réception des données
- Temps de surveillance F pour la communication F
- UUID de communication F
- Variables pour l'envoi des données
- Variables pour la réception des données

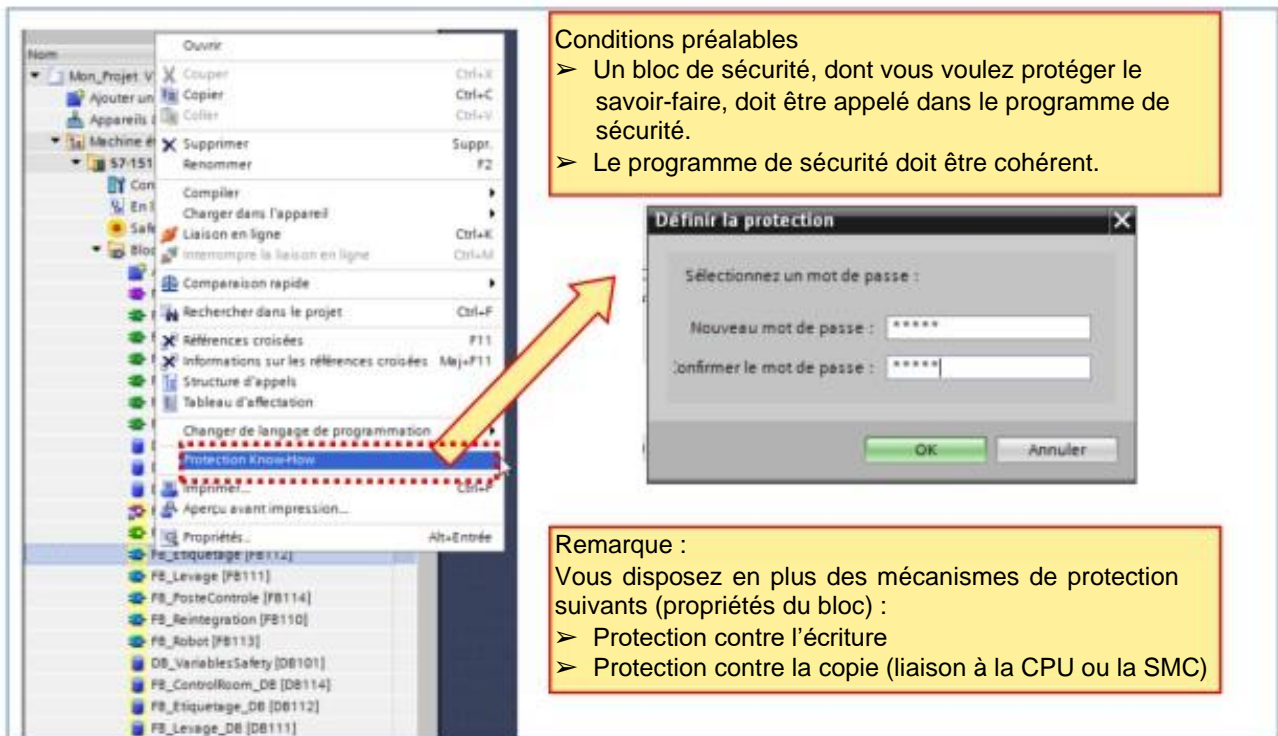
Générer un nouveau UUID de communication F

Sélectionnez la ligne entière et confirmez « Générer UUID » dans le menu. Vous pouvez également générer plusieurs UUID simultanément.

Des informations supplémentaires sur le sujet du F-Link flexible sont disponibles dans le chapitre 7 « Communication de sécurité ».

6.7. Protection du savoir-faire

6.7.1. Mise en place



Conditions préalables

- Un bloc de sécurité, dont vous voulez protéger le savoir-faire, doit être appelé dans le programme de sécurité.
- Le programme de sécurité doit être cohérent.

Définir la protection

Sélectionnez un mot de passe :

Nouveau mot de passe : *****

Confirmer le mot de passe : *****

OK Annuler

Remarque :

Vous disposez en plus des mécanismes de protection suivants (propriétés du bloc) :

- Protection contre l'écriture
- Protection contre la copie (liaison à la CPU ou la SMC)

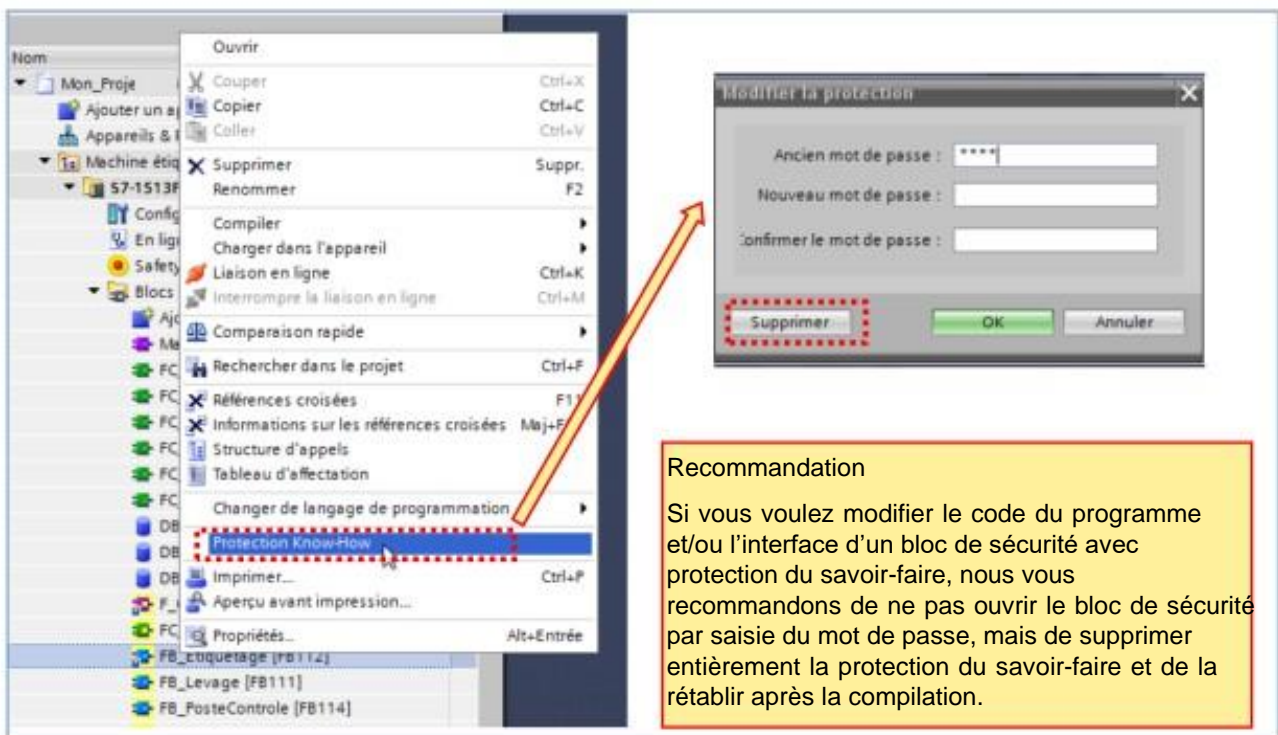
Conditions préalables :

- Un bloc de sécurité, dont vous voulez protéger le savoir-faire, doit être appelé dans le programme de sécurité.
- La protection du savoir-faire d'un bloc de sécurité ne peut être activée que si le programme de sécurité est cohérent. Pour ce faire, compilez le programme de sécurité.

Remarques :

- Aucun code source ne figure dans l'impression du programme de sécurité pour les blocs de sécurité avec protection du savoir-faire. Réalisez par conséquent une impression du programme de sécurité (par ex. pour la vérification du code ou pour la réception du bloc F) avant d'activer la protection du savoir-faire.
- Si vous voulez modifier le code programme et/ou l'interface d'un bloc F avec protection du savoir-faire, nous vous recommandons de ne pas ouvrir le bloc F par entrée du mot de passe, mais de supprimer entièrement la protection du savoir-faire et de la rétablir après la compilation.
- Lorsqu'un bloc de sécurité avec protection du savoir-faire ou des blocs de sécurité appelés par ce dernier sont renommés, la signature du bloc F avec protection du savoir-faire n'est modifiée qu'au moment de l'entrée du mot de passe à l'ouverture ou la suppression de la protection du savoir-faire.

6.7.2. Suppression



6.8. Compilation

6.8.1. Compiler le programme de sécurité (1)

Le programme de sécurité se compile suivant la même procédure qu'un programme standard.

Remarques concernant la compilation du programme de sécurité

Le programme de sécurité doit être recompilé après une modification de sécurité de la configuration matérielle,

Le programme de sécurité ne sera pas compilé de manière cohérente pour les conditions suivantes, :

- Si vous sélectionnez un répertoire créé par l'utilisateur dans l'arborescence du projet
- Si vous sélectionnez un ou plusieurs blocs de programme dans le répertoire « Program blocks » dans l'arborescence du projet

Utilisez ces préconisations pour vérifier la cohérence des blocs F modifiés.

Compiler un programme de sécurité

Pour compiler un programme de sécurité, vous devez globalement procéder comme pour la compilation d'un programme utilisateur standard. Différentes possibilités d'accès sont prévues à cet effet dans STEP 7. Quelle que soit la sélection, un contrôle de cohérence est toujours effectué. Ce contrôle de cohérence s'étend à tous les blocs sélectionnés. Si aucune erreur n'est détectée par le contrôle de cohérence, le statut du programme de sécurité compilé est cohérent.

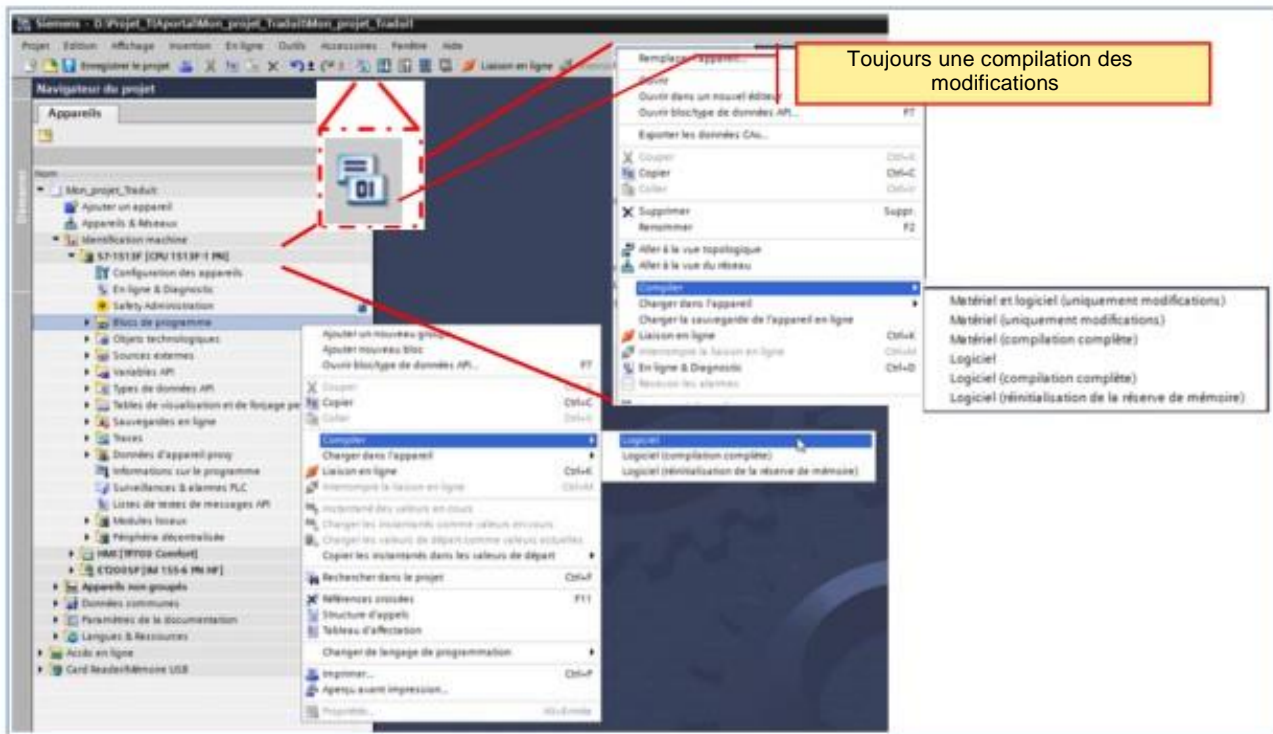
« Le programme de sécurité est cohérent »

Après une compilation réussie du programme de sécurité, un programme de sécurité cohérent se trouve toujours dans le dossier « Blocs de programme ». Il peut y avoir toutefois des blocs de sécurité qui ne sont pas appelés dans un groupe d'exécution d'une séquence de programme de sécurité. Ces blocs de sécurité s'affichent dans la rubrique « F-blocks » de l'éditeur Safety Administration, mais sont accompagnés d'un « Non » dans la colonne « Utilisé et compilé ».

Résultat « Le programme de sécurité n'est pas cohérent »

Si la compilation du programme de sécurité a abouti au résultat « Le programme de sécurité n'est pas cohérent », seuls les blocs de sécurité sélectionnés ont été compilés. Les blocs de sécurité et les blocs système de sécurité supplémentaires n'ont pas été générés. Le programme de sécurité du dossier « Blocs de programme » n'est pas cohérent et n'est donc pas exécutable.

6.8.2. Compiler le programme de sécurité (2)



Compiler le programme de sécurité

La cohérence du programme de sécurité hors ligne n'est assurée que si le programme de sécurité est entièrement compilé après chaque modification relative à la sécurité, que ce soit dans la configuration matérielle ou le paramétrage ou dans le programme de sécurité lui-même. Seul un programme de sécurité cohérent reçoit une signature hors ligne.

Logiciel (uniquement modifications)

Seuls les blocs modifiés du programme standard et du programme de sécurité sont compilés.

Logiciel (tous les blocs)

Tous les blocs du programme standard et du programme de sécurité sont compilés.

Signalement d'erreurs de compilation

Si la compilation s'est correctement déroulée, vous pouvez vérifier dans la fenêtre d'inspection, sous « Info > Compiler », si des messages d'erreur ou des avertissements ont été émis. Pour savoir comment corriger les erreurs de compilation, consultez la rubrique « Corriger les erreurs de compilation » dans l'Aide de STEP 7.

6.9. Charger dans la CPU

6.9.1. Charger le programme de sécurité dans la CPU (1)

Même procédure que pour le chargement d'un programme standard.

Remarques concernant le chargement du programme de sécurité

- Seuls le chargement cohérent ou le chargement de tous les blocs sont possibles
- Charger un programme de sécurité cohérent n'est possible qu'en mode STOP.
- Le programme de sécurité doit également être rechargé après une modification d'un paramètre de sécurité dans la configuration matérielle.

Charger le programme de sécurité

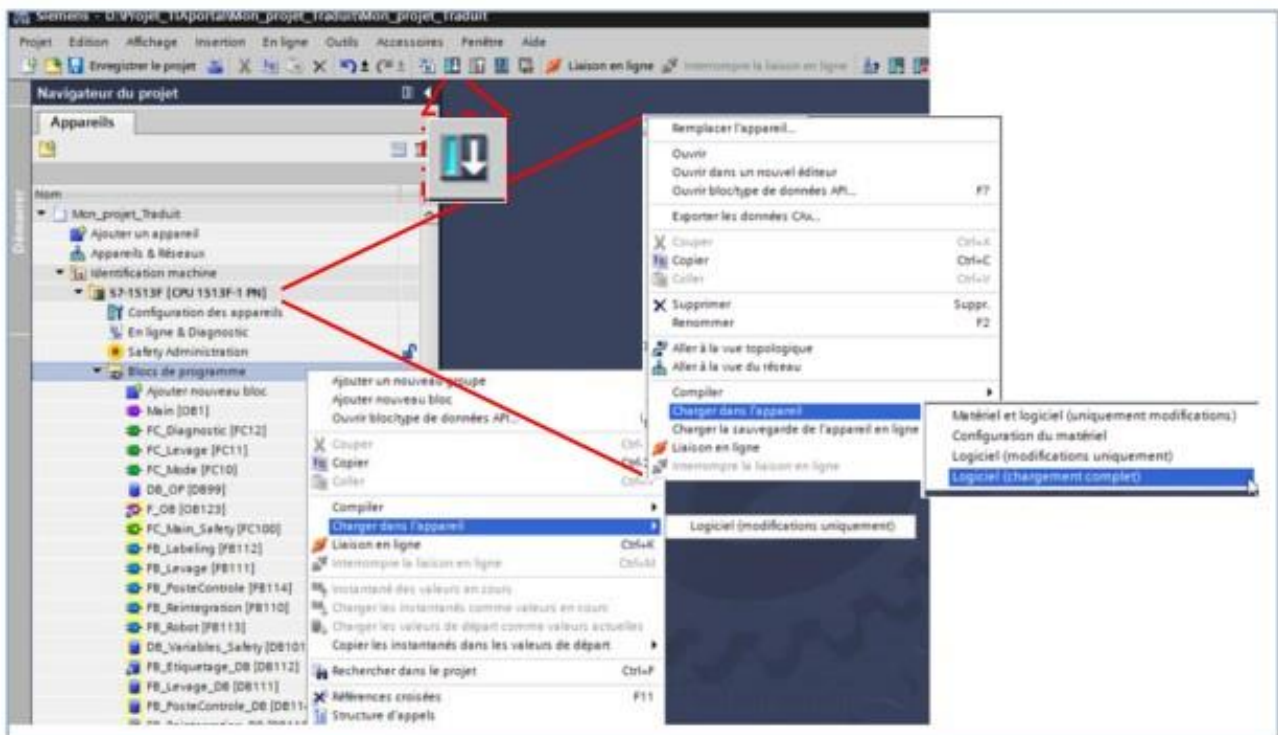
Pour charger un programme de sécurité, procédez de la même manière que pour charger un programme utilisateur standard en utilisant les différentes possibilités d'accès de STEP 7 :

- Dans la boîte de dialogue « Aperçu du chargement », entrez les données (par ex. mot de passe de la CPU F) et définissez les conditions préalables requises pour le chargement (par ex. mise à l'état STOP de la CPU F avant le chargement).
- Les résultats du chargement s'affichent dans la boîte de dialogue « Charger les résultats ».

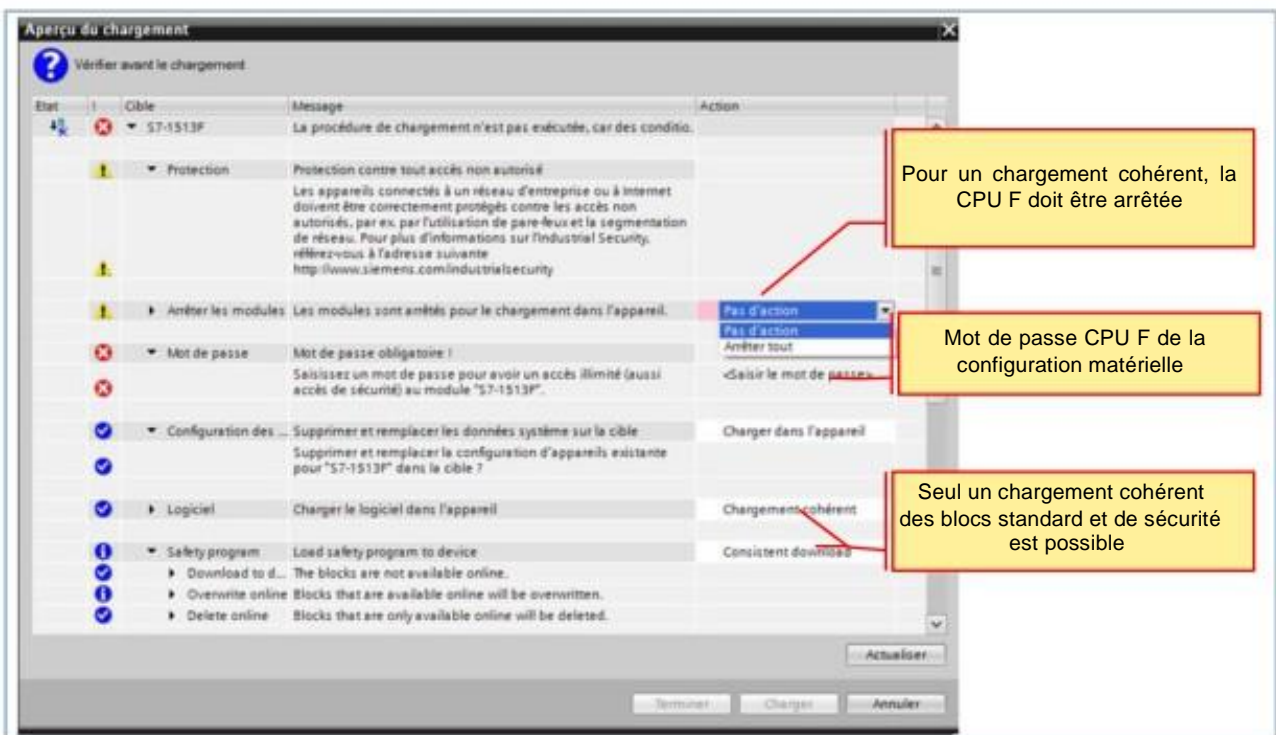
Charger le programme de sécurité dans la CPU

La cohérence du programme de sécurité de la CPU n'est assurée que si le programme de sécurité est entièrement compilé et chargé dans la CPU après chaque modification relative à la sécurité, que ce soit dans la configuration ou le paramétrage matériels ou dans le programme de sécurité lui-même. Cela n'est possible qu'à l'état STOP de la CPU. Seul un programme de sécurité cohérent se voit attribuer une signature en ligne.

6.9.2. Charger le programme de sécurité dans la CPU (2)



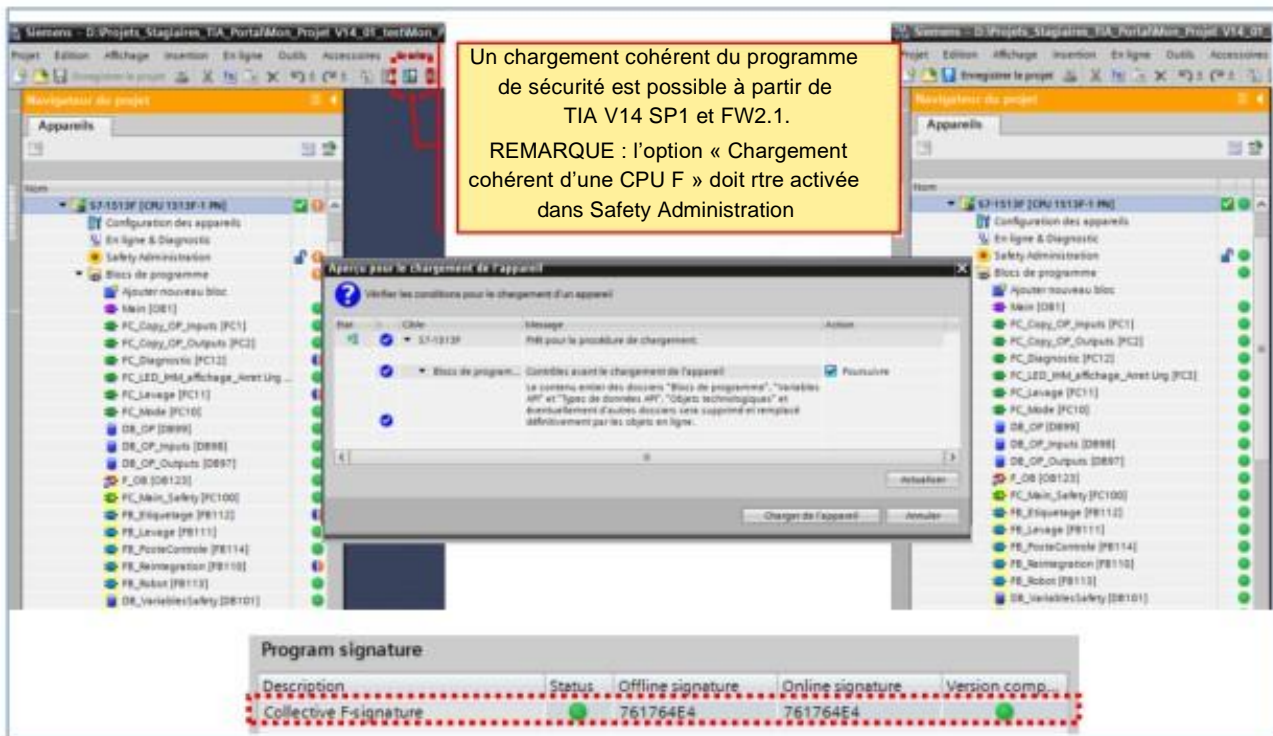
6.9.3. Charger le programme de sécurité dans la CPU (3)



Pour les CPU F S7-1200/1500, seule la valeur « Chargement cohérent » est disponible dans la boîte de dialogue « Aperçu du chargement ». Il n'est pas possible de sélectionner un chargement séparé du programme standard et du programme de sécurité. Dès que des modifications ont été effectuées dans le programme standard ou dans le programme de sécurité, le programme utilisateur global cohérent est automatiquement chargé.

6.10. Charger sur PG/PC

6.10.1. Charger le programme de sécurité sur PG/PC



Charger le programme de sécurité sur une PG / un PC (S7-1200, S7-1500)

La fonction « Chargement d'un appareil (logiciel) » ou « Chargement de l'appareil comme nouvelle station (matériel et logiciel) » n'est possible pour les CPU F S7-1500 que si l'option « Permettre un chargement cohérent depuis la CPU F » est activée dans l'éditeur Safety Administration et que les données projet ont été chargées dans la CPU F.

Pour charger les données projet (y compris les données projet de sécurité) dans un PG/PC, procédez comme pour un programme standard. Si plusieurs CPU F sont accessibles via un réseau (par ex. Industrial Ethernet) à partir de la PG / du PC, vous devez vous assurer que les données projet sont chargées à partir de la CPU F correcte. Par ex. avec « En ligne & Diagnostic » > « Accès en ligne » > « Clignotement des LED ». Une fois le chargement de l'appareil correctement effectué, vous pouvez poursuivre le traitement comme avec un projet créé hors ligne. Vous pouvez charger des blocs de sécurité individuels dans une PG / un PC indépendamment de l'option « Permettre un chargement cohérent depuis la CPU F ». Vous ne pouvez pas charger dans une PG / un PC des blocs de sécurité individuels avec protection du savoir-faire.

6.11. Tester le programme de sécurité

Modification des données du programme de sécurité par forçage de variables

Outre les données toujours forçables du programme utilisateur standard, vous pouvez modifier les données suivantes du programme de sécurité **en mode de sécurité désactivé** :

- Mémoire image des entrées et sorties de la périphérie F
- Variables dans les DB globaux de sécurité (F-DB) et les DB d'instance des F-FB

Remarque pour les tests :

- Le forçage d'entrées et de sorties de périphérie F (: P) n'est pas possible.
- Le forçage de sorties de périphérie F en liaison avec la fonction « Activation de sorties de périphérie F » n'est pas possible.
- La définition de points d'arrêt dans le programme utilisateur standard provoque des erreurs dans le programme de sécurité.

Tester le programme de sécurité

Après la création d'un programme de sécurité, vous devez effectuer un test de fonctionnement complet de votre tâche d'automatisation. Si vous modifiez un programme de sécurité ayant déjà subi un test de fonctionnement complet, il suffit de tester les modifications.

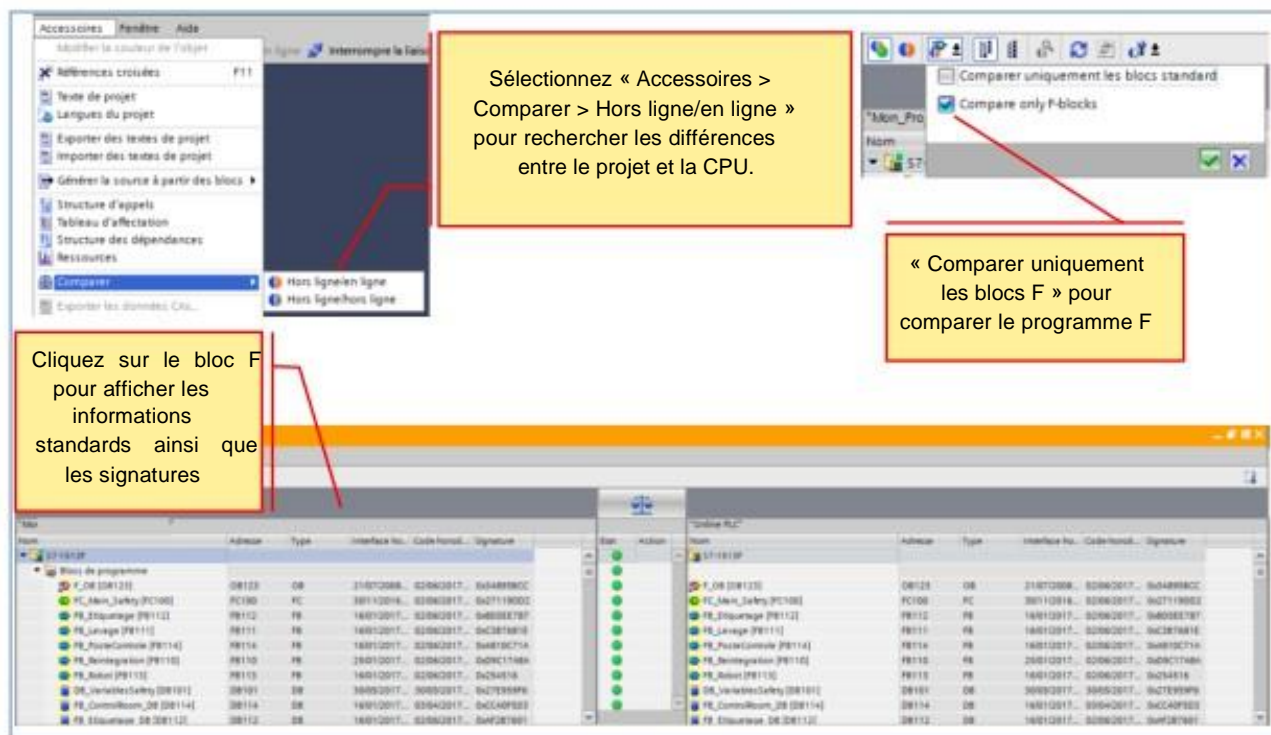
Visualiser

En principe, toutes les fonctions de test avec accès en lecture (par ex. visualisation de variables) sont également disponibles pour les programmes de sécurité en mode sécurité activé.

Forcer

Le forçage de données du programme de sécurité et les accès en écriture au programme de sécurité ne sont possibles que de manière limitée et en mode sécurité désactivé.

6.12. Comparer des programmes de sécurité



Comparer des programmes de sécurité

Vous pouvez comparer des programmes de sécurité hors ligne/en ligne ou hors ligne/hors ligne via l'éditeur de comparaison de STEP 7. La procédure est la même que pour les programmes utilisateur standard. Lors de la comparaison de programmes de sécurité, les contenus des blocs de sécurité sont également comparés. On peut donc utiliser une comparaison hors ligne/hors ligne pour la réception de modifications. Pour activer cette comparaison, activez le critère de comparaison « Safety » et désactivez tous les autres.

Résultat de la comparaison de programmes de sécurité

Les informations affichées indiquent si le programme de sécurité est cohérent. Si la liaison avec la CPU F est interrompue lors de la comparaison, le résultat de la comparaison sera incorrect.

Options de filtres pour la comparaison

En utilisant les filtres de l'éditeur de comparaison, vous pouvez limiter le résultat de la comparaison aux groupes de blocs suivants :

- Comparer uniquement les blocs de sécurité
- Comparer uniquement les blocs de sécurité pertinents pour la réception
- Comparer tous les blocs
- Comparer uniquement les blocs standard

Vous disposez en outre des deux options de filtre « Afficher uniquement les objets différents » et « Afficher les objets identiques et différents » de STEP 7. Pour la comparaison de programmes de sécurité, les blocs de sécurité du dossier « Blocs système » sont également pertinents.

Imprimer le résultat de la comparaison

Vous pouvez imprimer le résultat de la comparaison à l'aide des commandes « Projet > Imprimer » de la barre de menus ou de l'icône « Imprimer » de la barre d'outils. Sélectionnez « Imprimer objets/plage » « Tous » et « Propriétés » « Tous ».

6.13. Bloc de données : RTG1SysInfo

Nom	Type de données	Valeur de départ	Valeur de visualisation	Commentaire
1	Input			
2	MODE	Bool	FALSE	1 = deactivated safety mode
3	MODE	Bool	FALSE	1 = deactivated safety mode
4	TCYC_CURR	Dint	100	current cycle time of the F-runtime group in ms
5	TCYC_LONG	Dint	102	longest cycle time of the F-runtime group in ms
6	TRTG_CURR	Dint	2	current runtime of the F-runtime group in ms
7	TRTG_LONG	Dint	6	longest runtime of the F-runtime group in ms
8	T1RTG_CURR	Dint	0	current runtime in ms for further use
9	T1RTG_LONG	Dint	0	longest runtime in ms for further use
10	F_PROG_SIG	Dword	DW#16#B08C...	Collective F signature of the safety program
11	F_PROG_DAT	DTL	DTL#2017-05-04-08:41:58.898941300	Completion date of the safety program
12	F_RTG_SIG	Dword	DW#16#38C...	Collective F signature of the F-runtime group
13	F_RTG_DAT	DTL	DTL#2017-05-04-08:41:58.898941300	Completion date of the F-runtime group
14	VERS_STSAF	Dword	DW#16#1400...	Version label of STEP 7 Safety
15	InOut			
16	Static			

DB d'information sur le groupe séquentiel (RTG1SysInfo)

Le DB d'information sur le groupe séquentiel d'exécution du programme de sécurité met à votre disposition des informations centralisées sur chaque groupe séquentiel de sécurité et sur l'ensemble du programme de sécurité.

Un DB d'information sur le groupe séquentiel de sécurité est automatiquement créé lors de la création d'un groupe séquentiel d'exécution du programme de sécurité (F-runtime group). Un nom symbolique lui est attribué par le système, par ex. « RTG1SysInfo ». Vous pouvez modifier ce nom dans l'éditeur Safety Administration.

Vous avez accès au contenu du DB d'information sur le groupe d'exécution d'une séquence de programme de sécurité par un adressage « entièrement qualifié », soit de manière groupée via le type de données API (UDT) F_SYSINFO mis à disposition par le système F (par ex. « RTG1SysInfo.F_SYSINFO »), soit à partir d'informations individuelles (par ex. « RTG1SysInfo.F_SYSINFO.MODE »).

Remarque

Les données « T1RTG_CURR » et « T1RTG_LONG » ne sont actuellement pas prises en charge par STEP 7 Safety.

6.14. Spécificités du programme de sécurité (1)

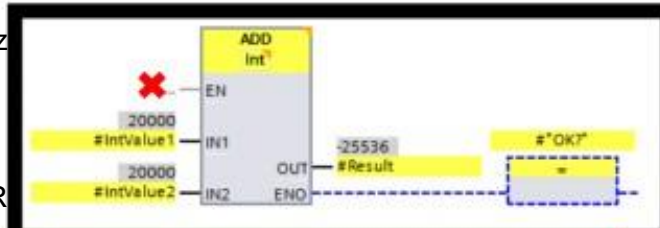
Enable input EN et enable output ENO

Enable input EN et enable output ENO ne sont pas utilisables.

Exception: (S7-1200, S7-1500):

Avec les instructions suivantes, vous pouvez connecter la sortie de validation ENO pour tester un dépassement de capacité :

ADD, SUB, MUL, DIV, NEG, ABS, CONVER

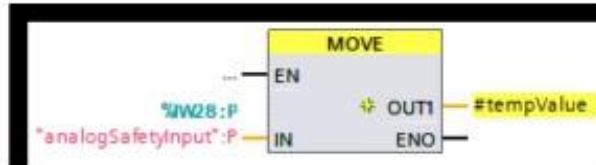


Si un dépassement de capacité n'est pas traité, des sorties de sécurité peuvent être falsifiées en fonction des équations logiques programmées. Cela provoquera un arrêt du traitement par Stop CPU!

Accès direct à la périphérie I/Q

Les I/Q sont uniquement adressables via la mémoire image dans le programme de sécurité.

L'accès direct aux I/Q n'est pas possible.



Autres restrictions

- L'accès Slice n'est pas possible dans le programme de sécurité.
- L'accès aux blocs non optimisés n'est pas possible avec les blocs de sécurité.
- Notez, lorsque vous utilisez la zone d'opérandes de données locales temporaires, que le premier accès d'un élément de données locales dans un bloc de sécurité principal F-FB/F-FC doit toujours être un accès en écriture. Cela permet d'initialiser l'élément de données locales.
- Il n'est pas possible d'accéder à des données locales statiques dans des instances uniques/multiples d'autres FB-F.

6.15. Spécificités du programme de sécurité (2)

Utilisation du type de données ARRAY et ARRAY[*]

- Uniquement les types de données INT et DINT
- Uniquement dans DB F globaux
- Limites pour ARRAY: 0 à maximum 10000
- ARRAY[*] uniquement possible en paramètre (InOut) dans les F-FC et F-FB

Uniquement accès en lecture dans le programme de sécurité avec les instructions:

RD_ARRAY_I
RD_ARRAY_DI

The screenshot displays two variable declaration tables and a ladder logic network.

MotorData Table:

	Name	Datentyp	Startwert
1	Static		
2	safeSpeed	Array[0..3] of Int	
3	safeSpeed[0]	Int	100
4	safeSpeed[1]	Int	200
5	safeSpeed[2]	Int	500
6	safeSpeed[3]	Int	1000

Motor Table:

	Name	Datentyp	Defaultwert
1	Input		
2	motorType	Dint	0
3	Output		
4	InOut		
5	safeSpeed	Array[*] of Int	
6	safeSpeed[*]	Int	

Netzwerk 1: Auswahl sichere Geschwindigkeit

Commentar:

```

graph TD
    RD_ARRAY_I[RD_ARRAY_I]
    EN[EN] --> RD_ARRAY_I
    RD_ARRAY_I --> OUT[OUT]
    OUT --> tempSafeSpeed[#tempSafeSpeed]
    tempSafeSpeed --> safeSpeed[#safeSpeed]
    safeSpeed --> ARRAY[ARRAY]
    ARRAY --> ERROR[ERROR]
    ERROR --> error[#error]
    error --> motorType[#motorType]
    motorType --> INDEX[INDEX]
    INDEX --> ENO[ENO]
  
```


6.16. Echange des données entre le programme standard et le programme de sécurité

Sont autorisés dans le programme standard :

- l'accès en lecture aux données de sécurité comme :
 - les blocs de données de sécurité
 - la mémoire image des modules F
- les évaluations des états de signaux et de fonctionnement courants
- **L'accès en écriture aux données F n'est pas autorisé**

Sont autorisés dans le programme de sécurité :

- l'accès en lecture OU en écriture aux données standard comme :
 - les blocs de données
 - la mémoire image standard
 - (les mémentos)
- **Les données standard ne doivent pas être modifiées pendant toute la durée du programme de sécurité → peut entraîner des altérations de données et une mise à l'état STOP de la CPU**

Transfert de données du programme de sécurité vers le programme utilisateur standard

Le programme utilisateur standard peut lire toutes les données du programme de sécurité, par ex. via des accès symboliques (entièrement qualifiés) :

- aux DB d'instance des F-FB (« "Nom DB Instance".Signal.x »)
- aux F-DB (par ex. « "Nom F_DB".Signal_1 »)
- à la mémoire image des entrées et sorties de la périphérie de sécurité (par ex. « "Arrêt_urgence_1" » (I 5.0))

Transfert de données du programme utilisateur standard vers le programme de sécurité

Dans le programme de sécurité, il n'est possible de traiter par principe que des données de sécurité ou des signaux de sécurité issus de la périphérie de sécurité et d'autres programmes de sécurité (dans d'autres CPU F), car toutes les variables du programme standard ne sont pas sécurisées.

Si vous devez toutefois traiter des variables issues du programme utilisateur standard dans le programme de sécurité, vous pouvez évaluer soit des mémentos du programme utilisateur standard, des variables d'un DB standard ou la mémoire image des entrées (MIE) de la périphérie standard dans le programme de sécurité (voir également le tableau des pages d'opérandes prises en charge au chapitre « Restrictions dans les langages de programmation LOG/CONT »).

Attention : les modifications structurelles des DB standard utilisés dans le programme de sécurité peuvent entraîner des incohérences du programme de sécurité et conduire, le cas échéant, à une demande de mot de passe. Après la compilation, la signature globale F correspond dans ce cas à nouveau à la signature d'origine. Pour éviter cet effet, utilisez des « blocs de données de couplage » entre le programme utilisateur standard et le programme de sécurité.

6.17. Accès à la mémoire image

		A partir du programme standard		A partir du programme de sécurité	
		lecture	écriture	lecture	écriture
Mémoire image standard	Entrées	✓	✓	✓	✗
	Sorties	✓	✓	✗	✓
Mémoire image de sécurité	Entrées	✓	✗	✓	✗
	Sorties	✓	✗	✗	✓

6.18. Accès aux blocs de données

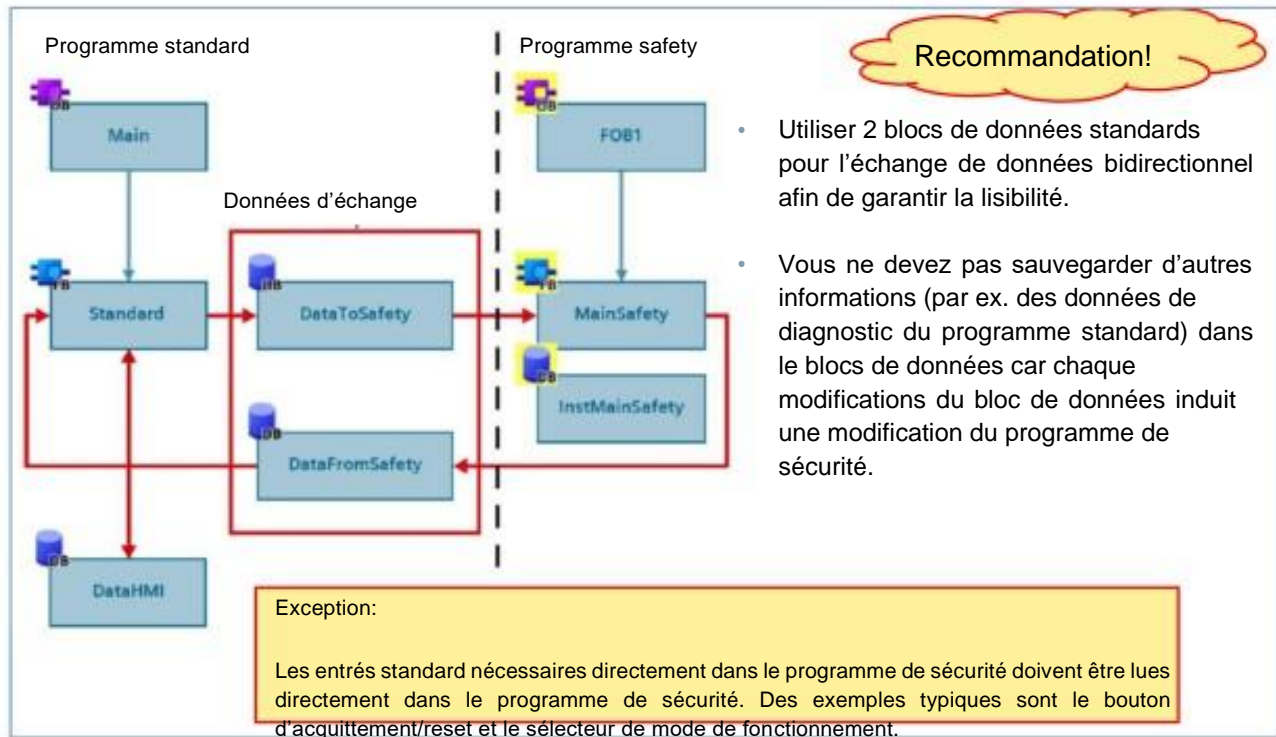
	À partir du programme standard		A partir du programme de sécurité	
	lecture	écriture	lecture	écriture
Bloc de données standard	✓	✓	<div> <div>✓</div> <div>✗</div> </div>	<div> <div>✗</div> <div>✓</div> </div>
Bloc de données de sécurité	✓	✗	✓	✓

Bloc de données/mémentos

Pour que les données du programme de sécurité puissent être directement écrites dans le programme utilisateur standard (par ex. sortie DIAG de l'instruction SENDDP), vous pouvez écrire des blocs de données du programme utilisateur standard dans le programme de sécurité. Une variable écrite ne peut cependant pas être lue dans le programme de sécurité.

Vous pouvez également écrire des mémentos dans le programme de sécurité. Un memento écrit ne peut cependant pas être lu dans le programme de sécurité.

6.19. Recommandation pour l'échange de données entre programme utilisateur standard et programme de sécurité



Avantages

- Groupe d'exécution F-runtime réduit
- Meilleure vue d'ensemble des données échangées
- Les modifications du concept de diagnostic et de signalisation dans le programme utilisateur standard n'affectent pas la signature du programme de sécurité
- Réduction des risques de temps d'arrêt dus à la corruption des données en raison de l'accès en écriture au programme de sécurité
- Saisie simplifiée des blocs F
- Les modifications apportées au programme utilisateur standard peuvent être chargées sans arrêter la CPU
- Le programme utilisateur standard et le programme de sécurité peuvent être créés indépendamment l'un de l'autre, à condition que des interfaces aient déjà été définies

Utilisation d'entrées non sécuritaires dans le programme de sécurité

Les entrées standard qui sont requises directement dans le programme de sécurité doivent être lues directement dans le programme de sécurité. Un « détournement » par le programme utilisateur standard doit être évité.

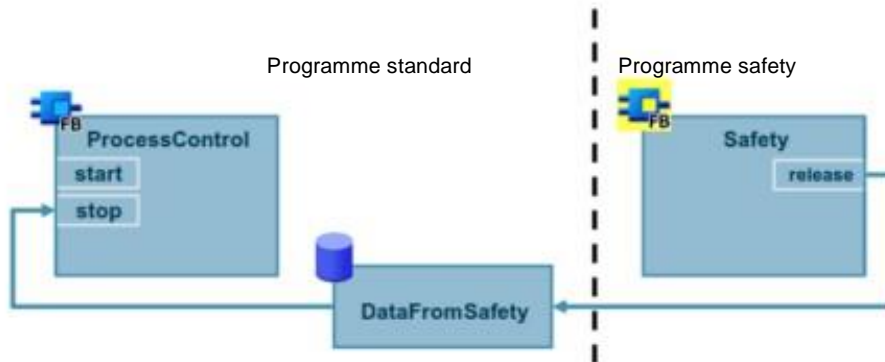
En effet, des signaux non liés à la sécurité sont également inclus dans l'intégrité systématique de l'application. Des exemples typiques sont les boutons d'acquiescement / de réinitialisation ou les sélecteurs de mode. Le choix du bouton / interrupteur autorisé pour réinitialiser une fonction de sécurité est un résultat direct de l'évaluation des risques. Une modification des dispositifs de commande doit donc influencer la signature et ne doit être effectuée qu'accompagnée d'une réévaluation des risques et d'un test de validation des modifications.

6.20. Réinitialisation de la commande opérationnelle

Les normes en vigueur exigent qu'une réinitialisation de la fonction de sécurité ne provoque pas de redémarrage de la machine.

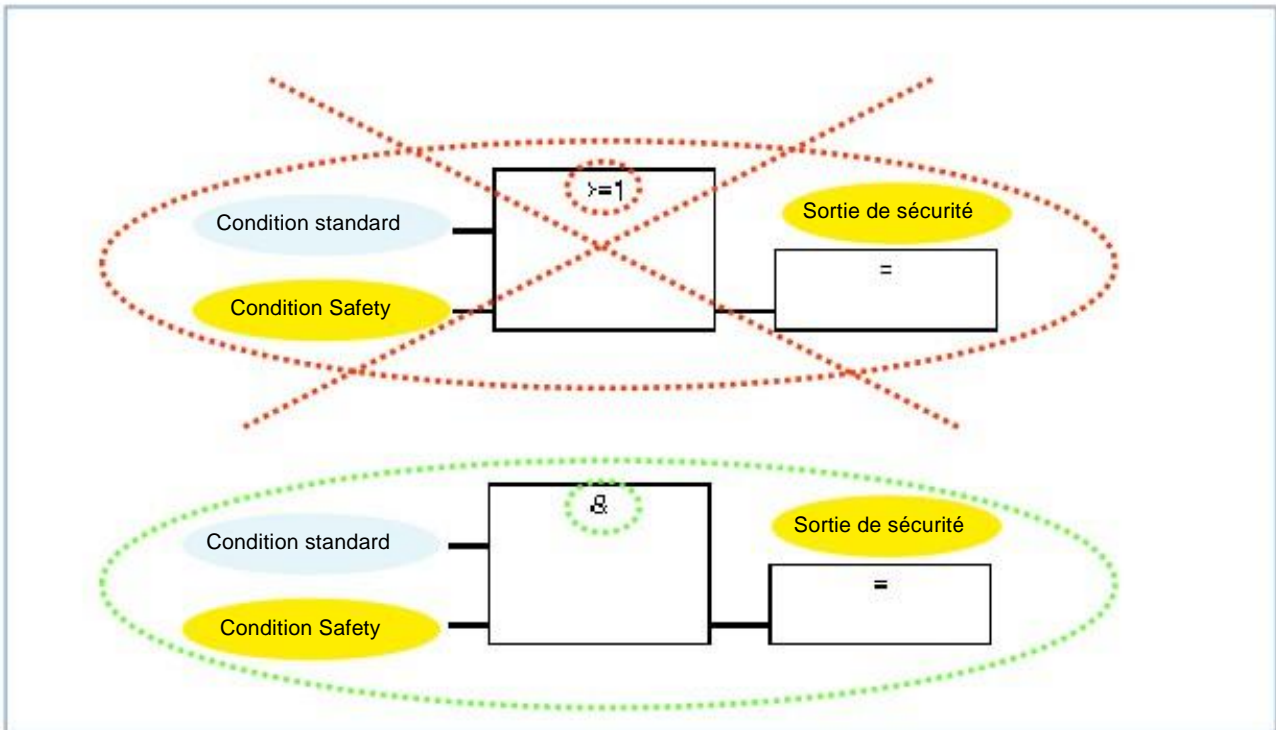
Recommandation!

- Verrouillez le processus de pilotage du programme standard avec un signal de validation issu du programme de sécurité. Ainsi un arrêt de sécurité entraîne également un arrêt du pilotage du processus.
- Transférez le signal de validation issu du programme de sécurité en utilisant un bloc de données global.



Des actionneurs de sécurité sont souvent utilisés pour la commutation opérationnelle. Les normes de sécurité applicables exigent qu'une réinitialisation de la fonction de sécurité ne déclenche pas le redémarrage de la machine. Lorsque la fonction de sécurité est déclenchée, la commutation de fonctionnement doit donc être réinitialisée et une nouvelle mise en marche doit être demandée.

6.21. Contrôle de plausibilité



Programmer les tests de plausibilité

- Utilisez les instructions de comparaison pour vérifier si les variables du programme utilisateur standard dépassent ou non les limites haute et basse autorisées. Vous pouvez ensuite influencer votre fonction de sécurité avec le résultat de la comparaison.
- Utilisez la fonction ---(S)--- : Set de la sortie, ---(R)--- : reset de la sortie ou SR : bascule SR, par exemple, avec des variables du programme utilisateur standard pour permettre de couper un moteur mais pas de le remettre en route.

Pour les opérations de mise en marche, combinez des variables du programme utilisateur standard à l'aide par ex. d'une opération ET avec des conditions de mise en marche issues de variables de sécurité.

Ces variables ne sont pas générées de manière sécuritaire, il faut s'assurer par des contrôles de plausibilité complémentaires dans le programme de sécurité que des états dangereux ne puissent apparaître. Si vous utilisez un memento, une variable d'un DB standard ou une entrée de la périphérie standard dans les deux groupes d'exécution F, alors il faut réaliser le contrôle de plausibilité dans chaque groupe séparément.

6.22. Exercice 1: Configurer le Touchpanel



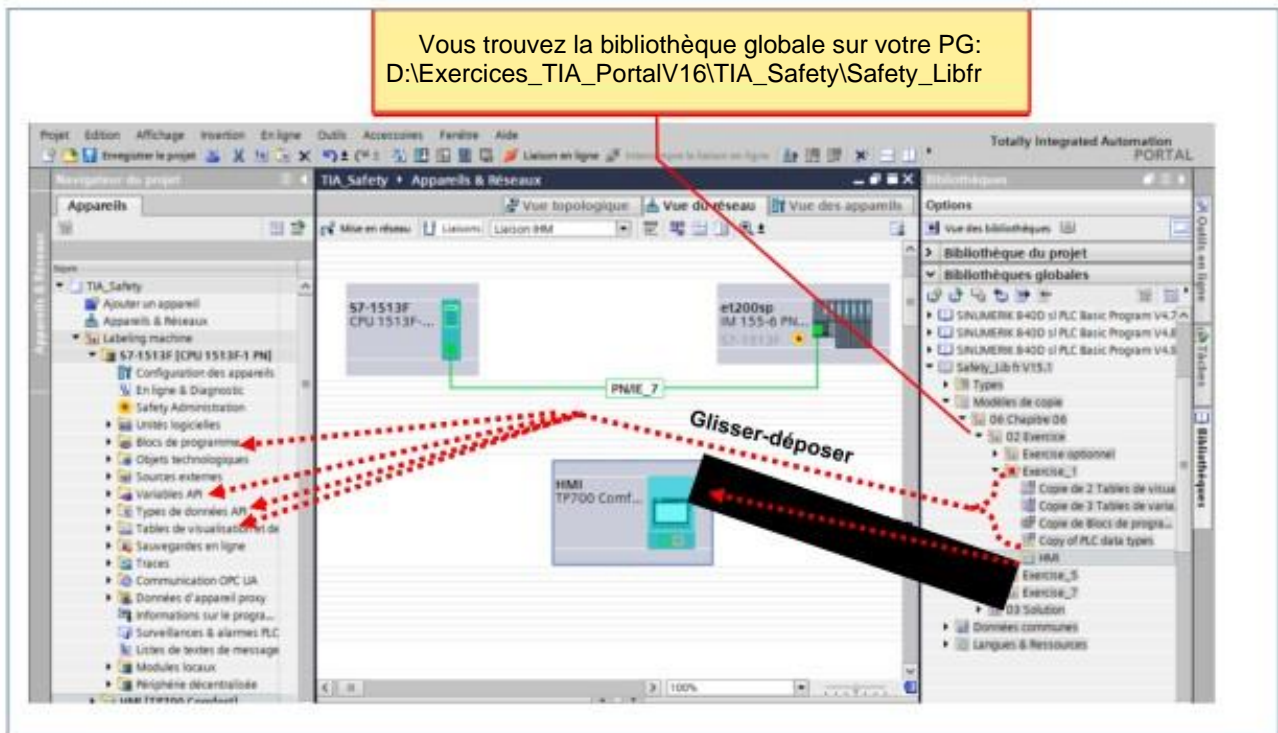
Enoncé

Votre projet ne contient pas encore d'interface homme machine. Plutôt que de procéder à une nouvelle configuration complète, vous allez utiliser un projet IHM préconfiguré ainsi que les blocs de programme nécessaire qui serviront d'interface entre l'automate et le Touchpanel à partir de la bibliothèque globale « Safety_Libfr ».

Marche à suivre

La marche à suivre est expliquée dans les pages suivantes.

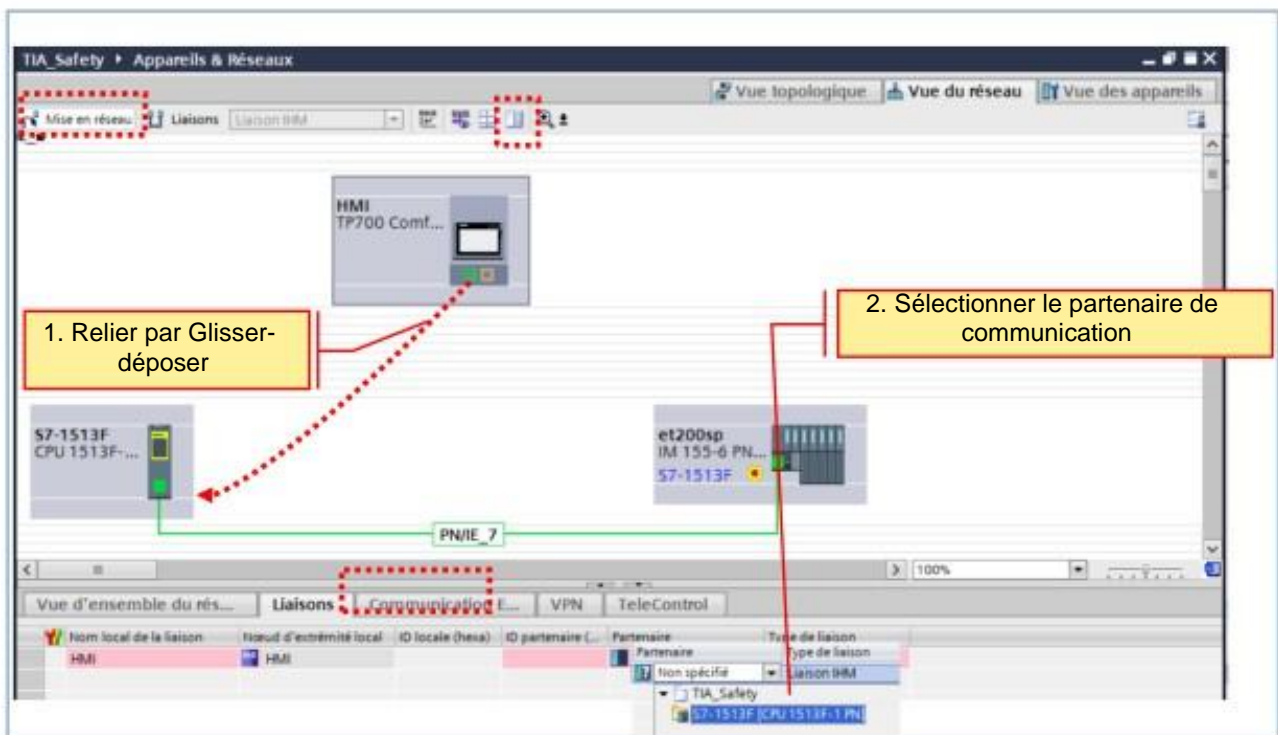
6.22.1. Exercice 1 : Copier le projet Touchpanel, le DB Interface et les FC de la bibliothèque



Procédure

1. Ouvrez la bibliothèque globale
« D : \ Exercices_TIA_PortalV16\ TIA_SAFETY\ Safety_Libfr »
2. Copiez par glisser-déposer les éléments de la bibliothèque à l'emplacement correspondant de votre projet (voir figure)
3. Copiez par glisser-déposer l'IHM
4. Enregistrez votre projet

6.22.2. Exercice 1 : Adapter la connexion de l'IHM



Énoncé

L'écran tactile ajouté doit à présent être mis en réseau et connecté hors ligne au réseau Ethernet.

Procédure

1. Lancez l'éditeur « Appareils & Réseaux » dans le Navigateur du projet, allez dans la « Vue du réseau », puis sélectionnez « Liaisons ».
2. Placez le pointeur de la souris sur l'interface Ethernet de l'appareil IHM et tracez une liaison avec la CPU en maintenant le bouton gauche de la souris. La liaison est établie, le sous-réseau correspondant et les paramètres destinés à la mise en réseau (adresse IP et masque de sous-réseau) sont automatiquement créés.
3. Si l'adresse IP courante de l'appareil IHM ne correspond à aucun sous-réseau de la CPU, le sous-réseau doit être sélectionné.

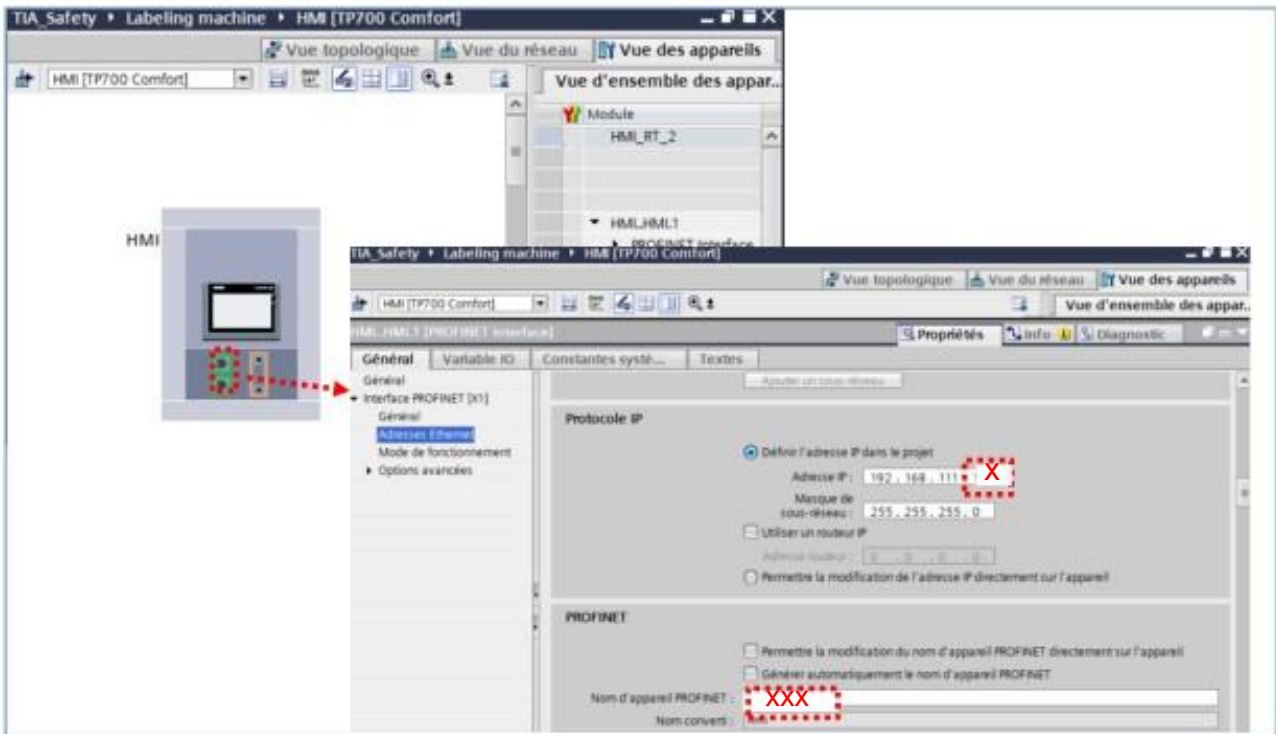
Note :

Dans le réglage de base, la vue du réseau tabellaire est souvent représentée miniaturisée à droite de la vue graphique du réseau.

Avec « Basculer l'orientation du fractionnement » vous pouvez commuter le fractionnement entre horizontal et vertical pour une meilleure visibilité.



6.22.3. Exercice 1 : Adapter l'adresse IP et le nom d'appareil PROFINET



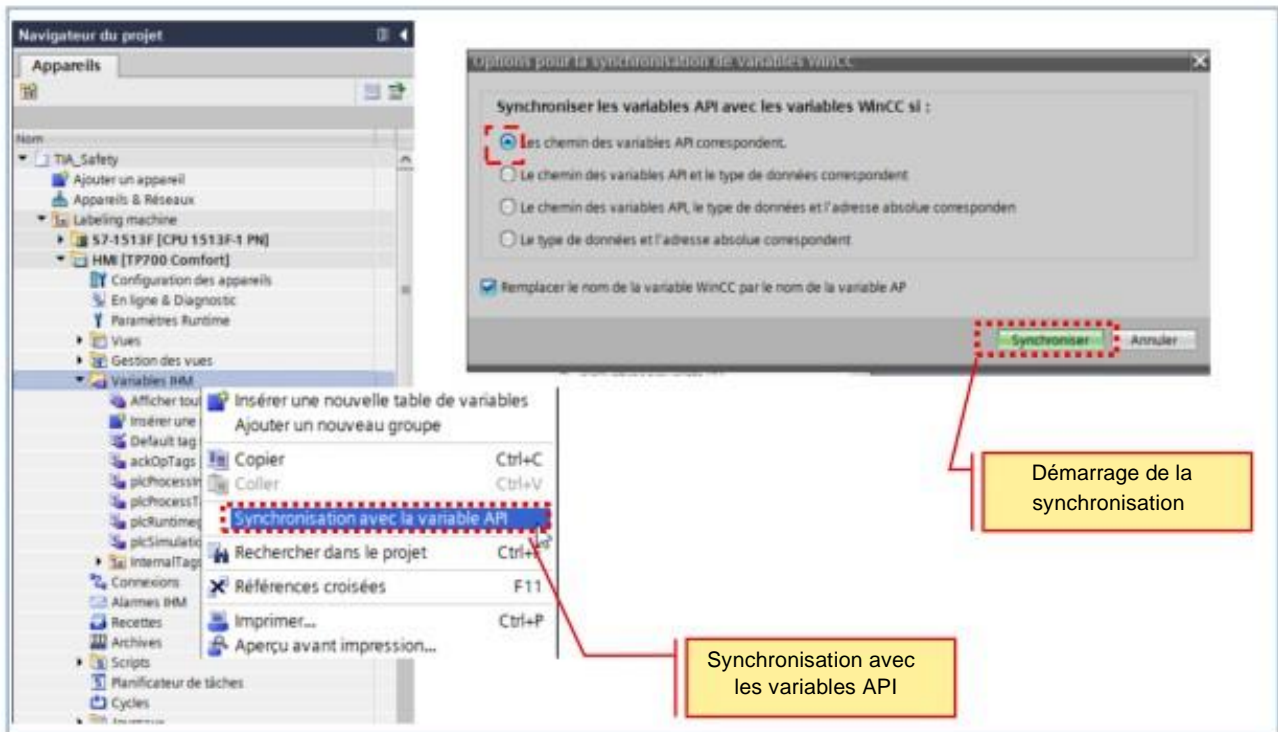
Énoncé

Une fois l'écran tactile mis en réseau et connecté, vous devez vérifier la liaison et adapter l'adresse IP et le nom PROFINET.

Procédure

1. Attribuez à l'écran tactile l'adresse IP qui figure sur le feuillet joint à la valise. Ce paramétrage peut être effectué via l'onglet « Propriétés » de la fenêtre d'inspection.
2. Attribuez en outre le nom d'appareil PROFINET qui figure sur le feuillet joint à la valise. Vous pouvez également le laisser générer à partir du nom de la station via « Générer automatiquement le nom d'appareil PROFINET » ou manuellement par suppression de la coche.

6.22.4. Exercice 1 : Synchroniser les variables IHM et API et compiler



Énoncé

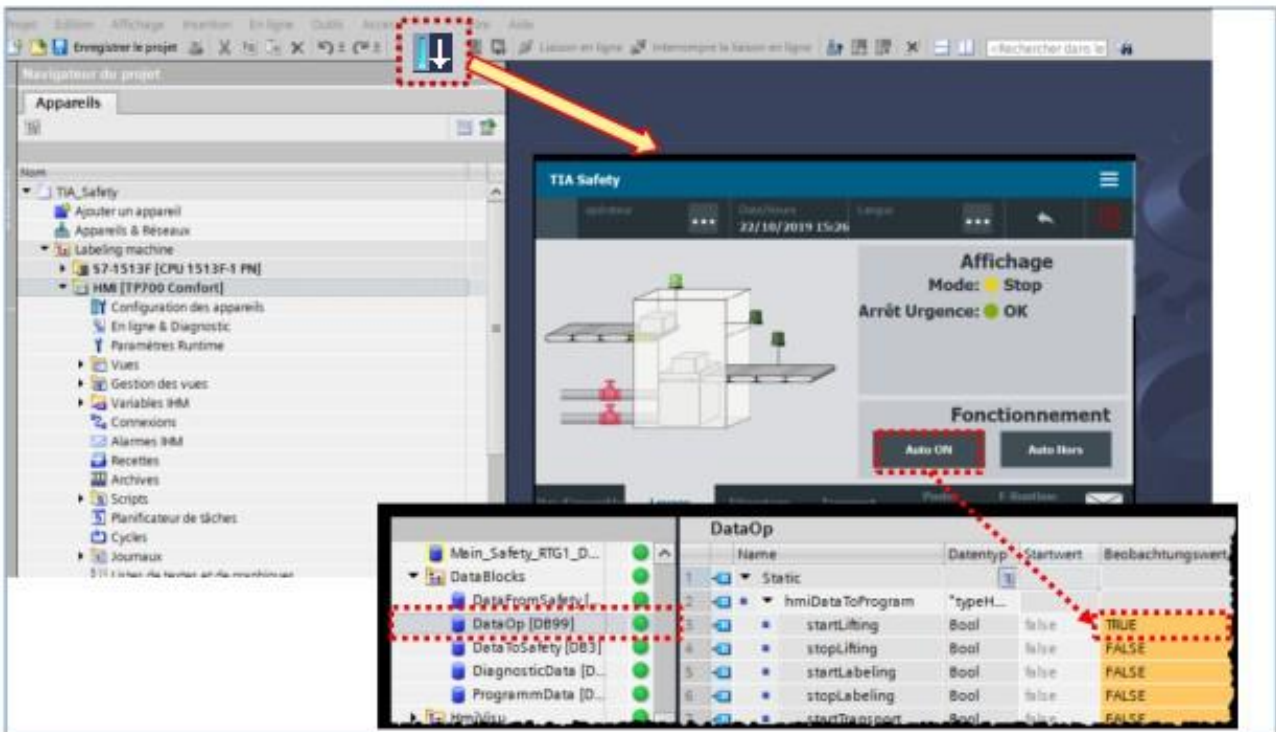
Les variables IHM sont repérées en rouge, car la liaison entre les variables API et les variables IHM n'est pas correcte. Votre tâche consiste maintenant à réaliser une synchronisation entre les variables IHM et les variables API.

Procédure

1. Ouvrez les « Variables IHM » de l'appareil IHM
2. Corrigez les liaisons erronées de manière qu'il ne subsiste plus aucune entrée rouge dans la table des variables

Astuce : modifiez la première liaison erronée, puis utilisez cette modification pour toutes les autres variables (cf. : Excel)
3. Synchronisez ensuite les variables WinCC (voir figure)
4. Compilation complète du projet IHM (matériel et logiciel)
5. Enregistrez votre projet

6.22.5. Exercice 1 : Chargement de l'IHM et de la CPU



Énoncé

Les projets IHM et CPU désormais terminés doivent être chargés.

Procédure

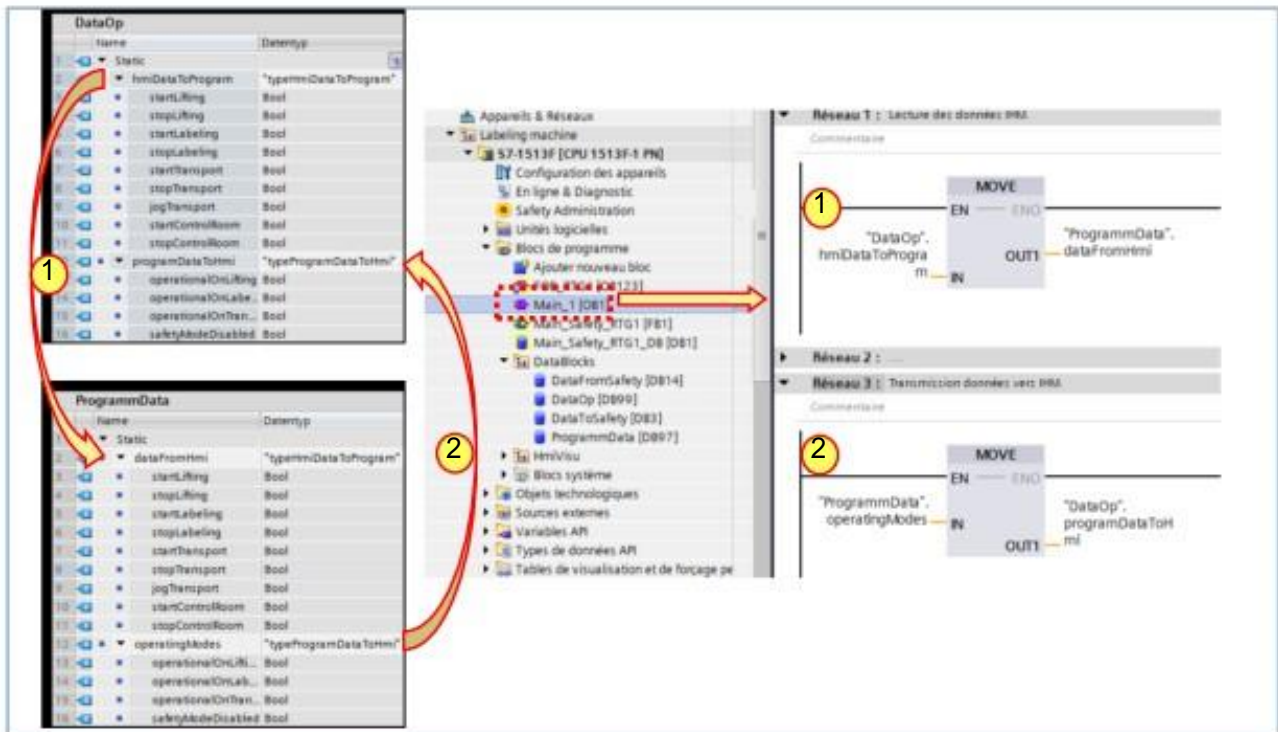
1. Chargez la CPU
2. Chargez l'IHM
3. Enregistrez le projet

Résultat

L'écran tactile doit à présent être relié à votre CPU. Vous pouvez visualiser les variables CPU du bloc de données « DB_OP » à l'aide de l'écran tactile.

Pour vérifier le bon fonctionnement du système, affichez l'écran « Poste de contrôle » de l'écran tactile, puis cliquez sur le bouton « Marche ». En mode visualisation, la variable « Marche » doit prendre la valeur « 1 » dans le bloc de données « DB_OP » du dispositif de levage.

6.22.6. Exercice 1 : Assurer l'échange de données cohérent entre IHM et CPU



Enoncé

Afin de garantir la cohérence des données, les données écrites par l'IHM dans le programme utilisateur sont copiées dans une zone de données séparée (DB "ProgrammData") au début du cycle.

"DataOp".hmiDataToProgram → "ProgrammData".dataFromHmi

Les données qui sont lues/évaluées par l'IHM doivent être transférées dans la mémoire tampon de données correspondante (DB "DataOp") à la fin du programme.

"ProgrammData".operatingModes → "DataOp".programDataToHmi

Note : Les CPU S7-1200/1500 n'utilisent plus de point de contrôle de cycle (S7-300/400) pour la mise à jour des variables IHM. Les variables sont mises à jour en cours d'exécution.

Procédure

1. Programmez les transferts directement dans votre programme cyclique standard (OB1).



Lecture des données de l'IHM (premier réseau)

Transfert des données vers l'IHM (dernier réseau)

2. Sauvegardez votre projet.

6.23. Affichage « Mode de sécurité désactivé »



Enoncé

Procédez à la mise en place de la structure de base du programme de sécurité et évaluez la mode de fonctionnement de sécurité. Si le mode de sécurité est désactivé il faut que l'utilisateur en soit immédiatement averti via l'IHM (copie écran).

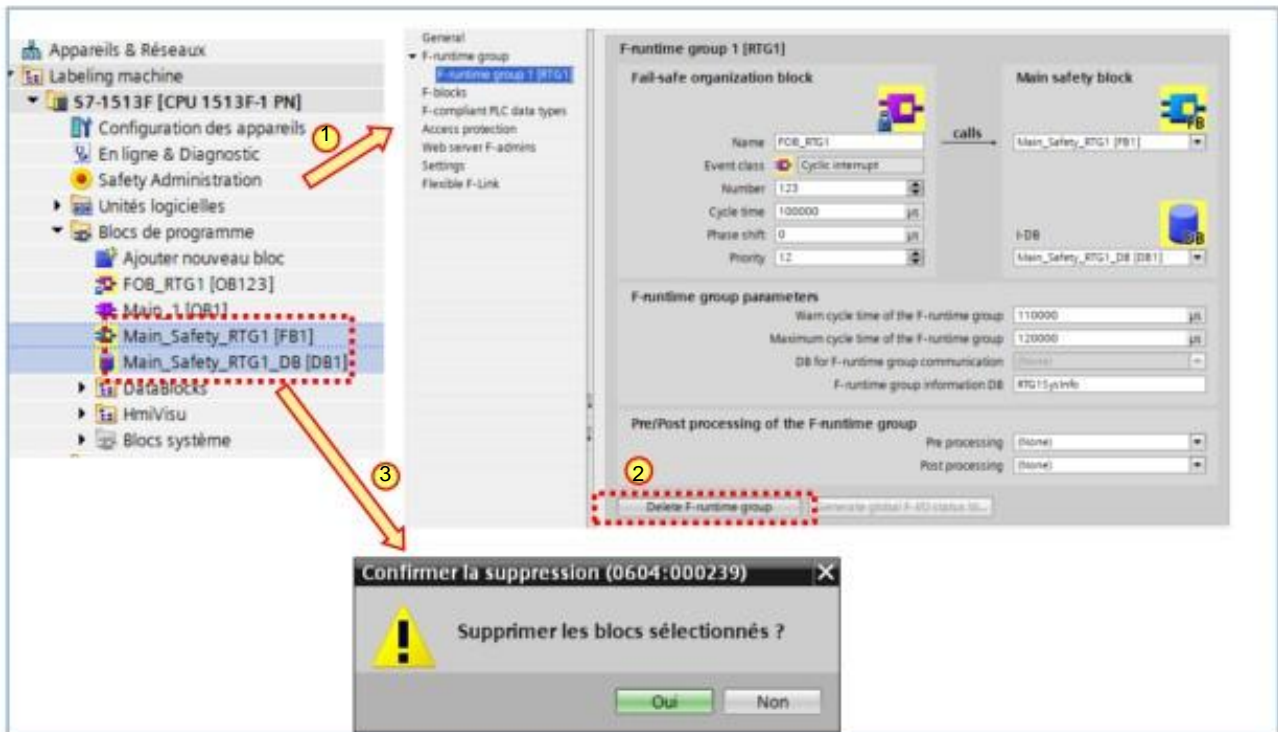
Remarque

L'affichage à l'IHM est préconfiguré et doit uniquement être piloté par le tampon de données.

Procédure

La procédure est expliquée dans les pages suivantes.

6.23.1. Exercice 2 : Effacer un groupe d'exécution existant

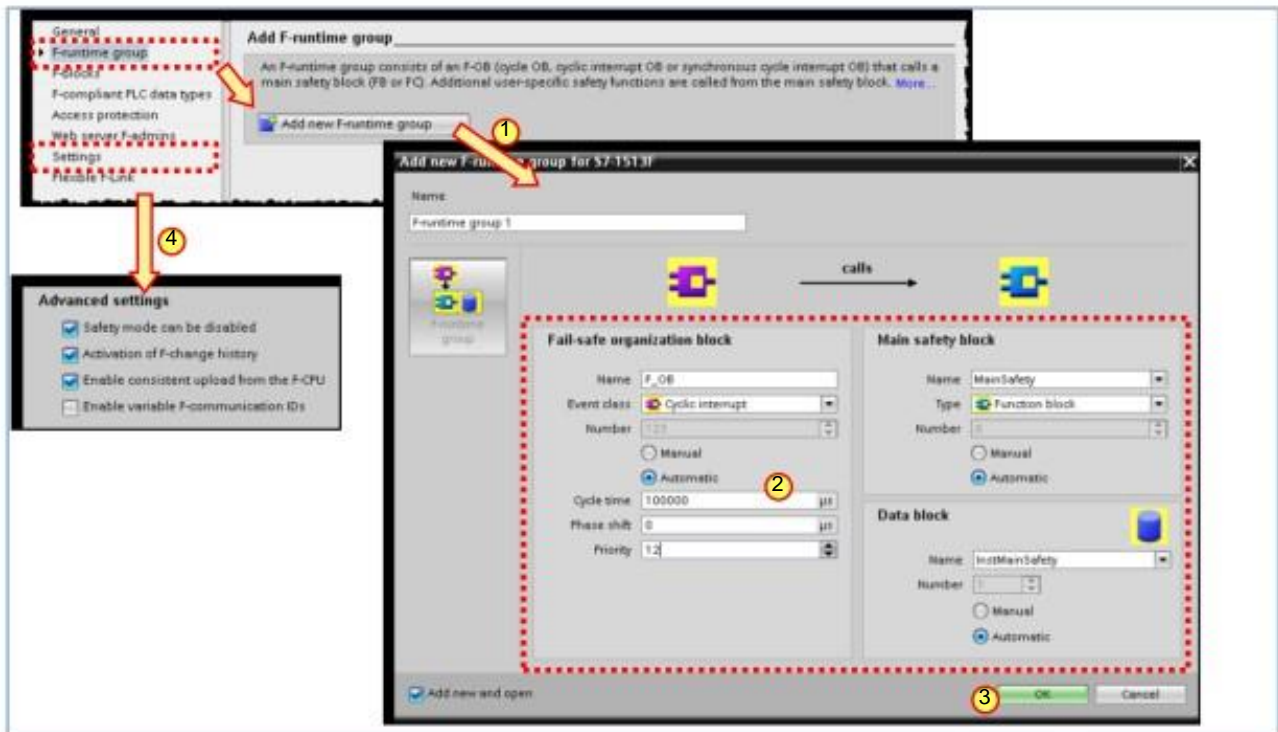


Un groupe séquentiel étant automatiquement créé lors de la création d'une CPU F dans le TIA Portal. L'effacement du groupe séquentiel créé automatiquement est uniquement réalisé à des fins d'exercice afin d'illustrer la création d'un nouveau groupe séquentiel.

Enoncé

1. Ouvrez le groupe séquentiel actuel « Safety Administration -> F-runtime group -> F-runtime group 1[RTG1] ».
2. Effacez le groupe d'exécution séquentiel du programme de sécurité.
3. Effacez les blocs F encore existants du groupe supprimé.
4. Enregistrez votre projet.

6.23.2. Exercice 2 : Création manuelle d'un nouveau groupe d'exécution



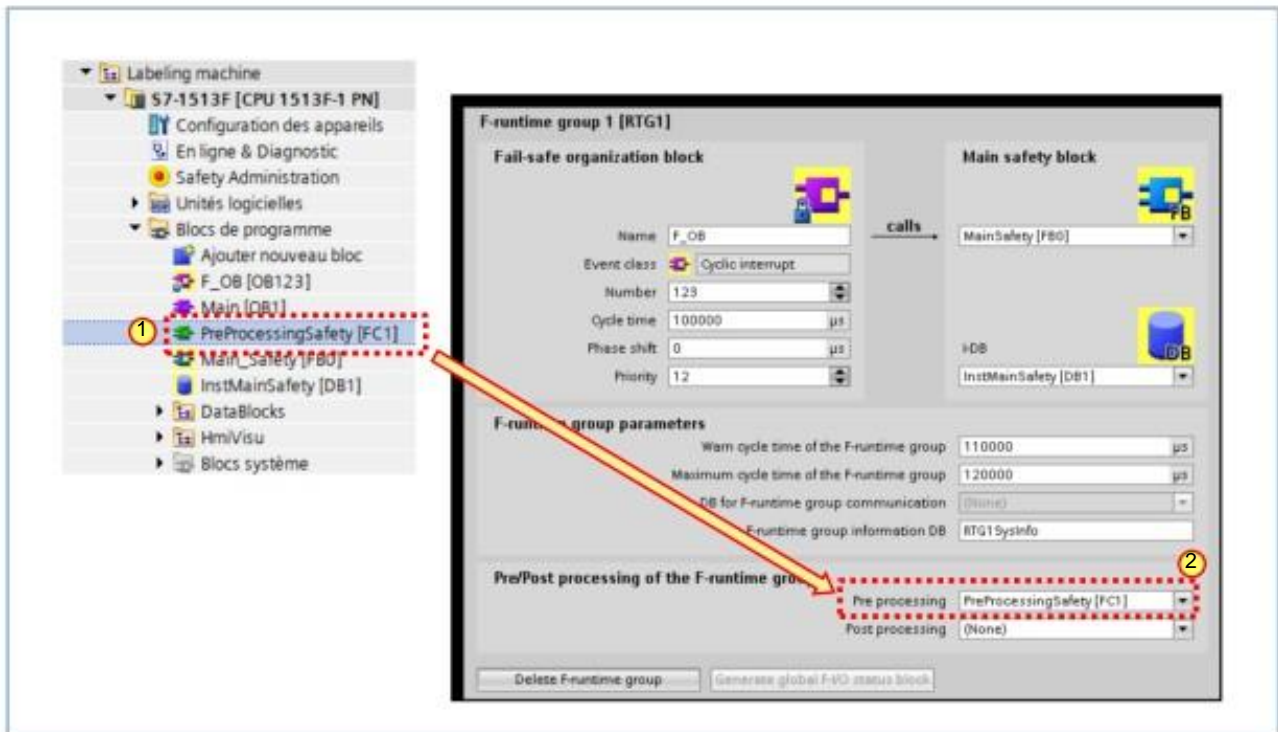
Énoncé

Vous devez à présent créer un nouveau groupe séquentiel. Ultérieurement celui-ci contiendra l'ensemble de votre programme de sécurité.

Procédure

1. Créez un nouveau groupe séquentiel
« Safety Administration -> F-runtime group -> Add new F-runtime group ».
2. Sélectionnez le nom et les paramètres comme indiqué sur la figure.
3. Configurez le groupe d'exécution séquentiel du programme de sécurité.
4. Activez l'option « Safety mode can be disabled »
« Safety Administration > Settings > Advanced settings ».
5. Enregistrez votre projet.

6.23.3. Exercice 2 : Création du Pre-processing d'un groupe d'exécution



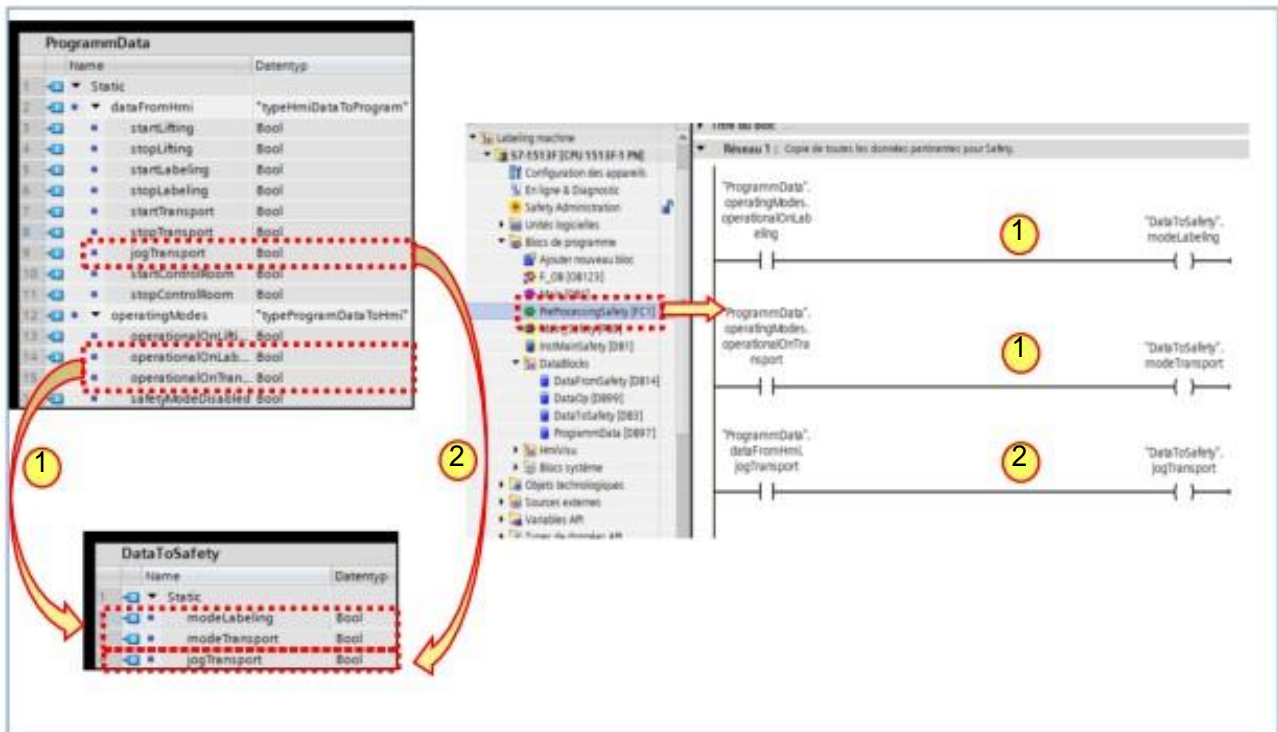
Enoncé

Pour garantir un transfert de données cohérent, une fonction de prétraitement du groupe d'exécution F doit être créée et affectée au groupe d'exécution.

Procédure

1. Créer une fonction standard « PreprocessingSafety ».
2. Associer la fonction au groupe d'exécution F existant en tant que prétraitement.
Note : Le post-traitement n'est pas nécessaire.
3. Sauvegardez votre projet.

6.23.4. Exercice 2 : transfert de données vers le programme de sécurité



Enoncé

Pour garantir un transfert de données cohérent, toutes les données standards qui seront nécessaires plus tard dans le programme de sécurité sont transférées dans le prétraitement du groupe d'exécution F.

Mode de fonctionnement de l'étiqueteuse :

```
"ProgrammData".operatingModes.operationalOnLabeling → "DataToSafety".modeLabeling
```

Mode de fonctionnement du transport :

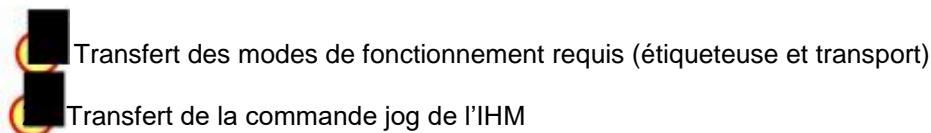
```
"ProgrammData".operatingModes.operationalOnTransport → "DataToSafety".modeTransport
```

Commande jog pour le transport :

```
"ProgrammData".dataFromHmi.jogTransport → "DataToSafety".jogTransport
```

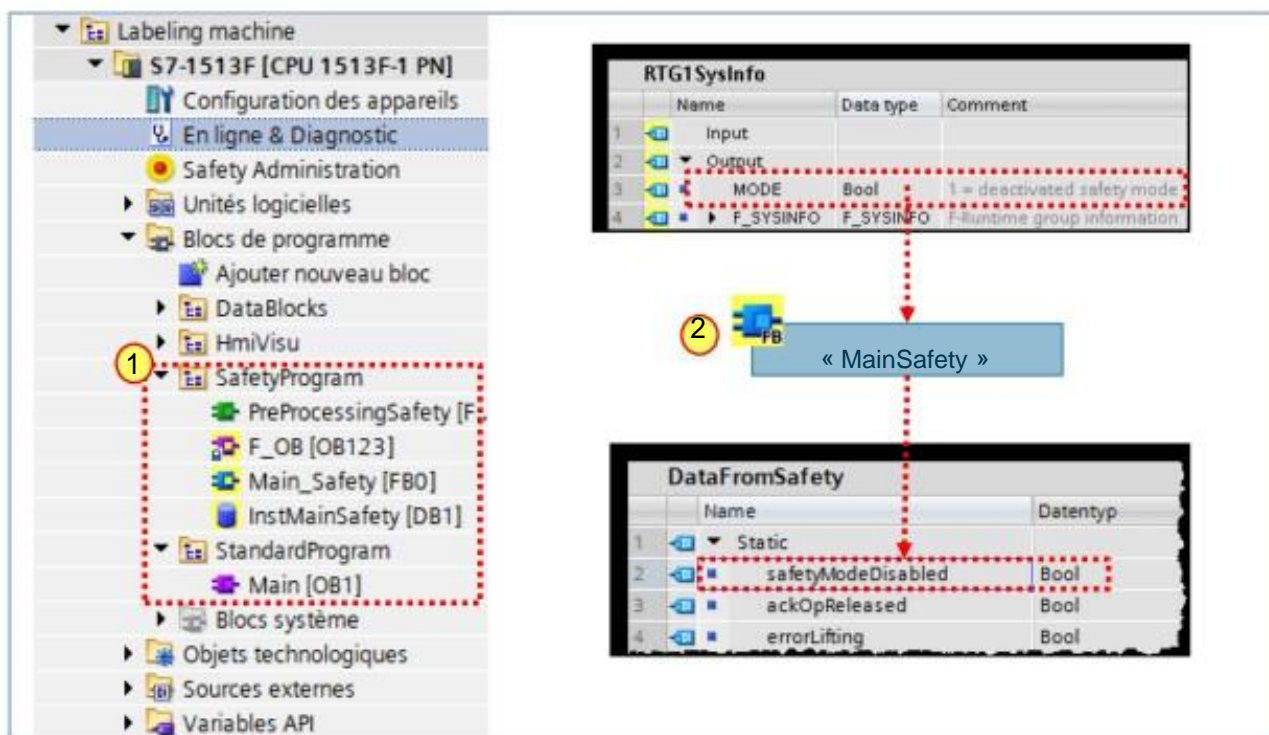
Procédure

Programmez le transfert de données directement dans votre fonction de prétraitement « "PreprocessingSafety" »



4. Sauvegardez votre projet.

6.23.5. Exercice 2 : définition des groupes de blocs et du « Main_Safety »



Enoncé

L'utilisateur doit être prévenu immédiatement en cas de désactivation du mode de sécurité de la CPU. Cet avertissement doit être réalisé au moyen d'un message affiché sur le Panel. Le regroupement judicieux des blocs de programme permettra une meilleure lisibilité du programme.

Procédure

1. Insérez un groupe de blocs pour le programme de sécurité « Programme de sécurité » et un autre pour le programme standard « Programme standard ». Déplacer les blocs concernés dans le répertoire respectif. (DB_OP.ModeSafetyDisabled) reste affiché tant que le mode de sécurité de la CPU est désactivé (RTG1SysInfo.MODE)
2. Programmez le « Main Safety » de telle manière que « Mode de sécurité désactivé » (DB "DataFromSafety" ModeSafetyDisabled) soit affiché tant que le mode de fonctionnement de sécurité soit désactivé sur la CPU (F-DB "RTG1SysInfo". MODE).

Note :

Le bloc système RTG1SysInfo se trouve dans le répertoire des blocs sous

« Blocs de programme > Blocs système > STEP 7 Safety »

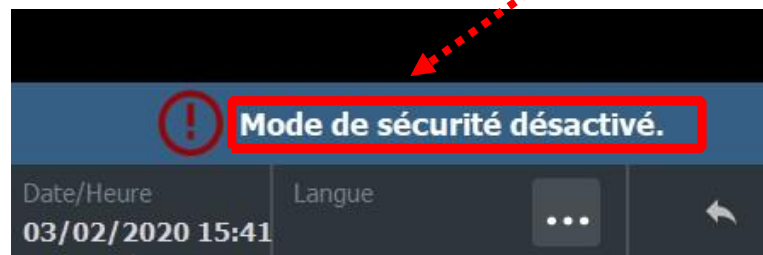
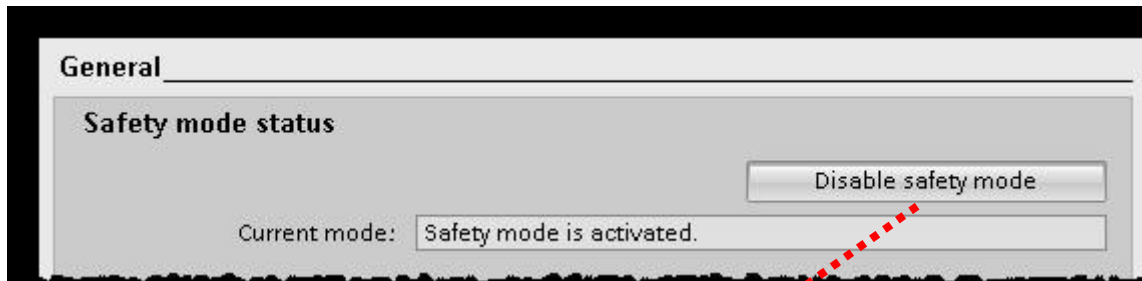
3. Charger les blocs dans la CPU.
4. Enregistrez votre projet

Interfaces concernées		
Blocs de données	Global	Système
	"DataFromSafety" ModeSafetyDisabled	"RTG1SysInfo".MODE

Suite page suivante

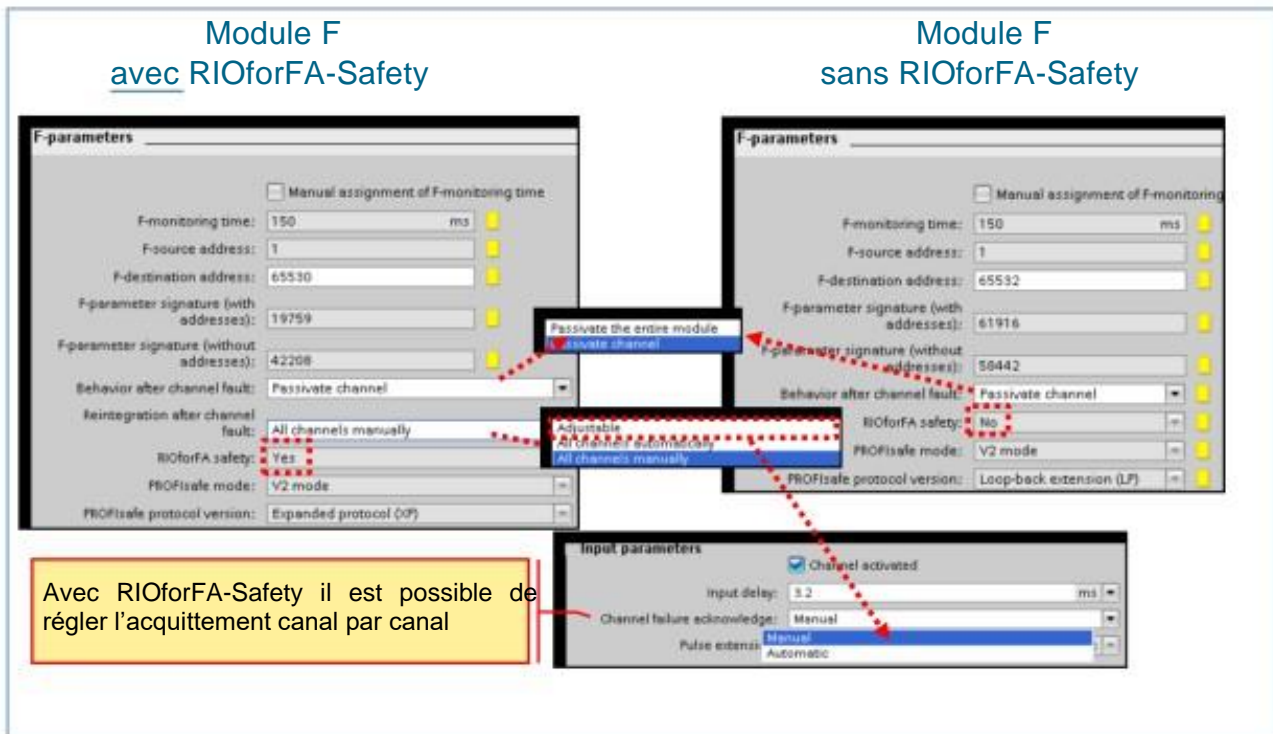
Résultat

La structure de base du programme de sécurité est maintenant créée, et le mode de sécurité désactivé est affiché à l'utilisateur sur l'IHM. Testez la fonctionnalité en désactivant le mode de sécurité dans « Safety Administration » et en vérifiant le message sur l'IHM.



6.24. Passivation des modules F

6.24.1. Principe



Passivation

Le concept de sécurité repose sur le principe qu'il existe un état de sécurité pour toutes les grandeurs du processus. Pour les modules de périphérie de sécurité, cette valeur de sécurité est l'état « 0 ». Lorsque le module de périphérie de sécurité détecte une erreur, il passive le canal concerné ou le module complet donc tous les canaux ce qui signifie que les canaux sont alors mis dans un état sûr.

La passivation d'un canal ou d'un module F peut intervenir...

- au démarrage du système F
- en cas d'erreurs de communication entre la CPU F et la périphérie de sécurité
- en cas de détection d'erreurs par la périphérie de sécurité (rupture de fil, court-circuit, court-circuit transversal...)
- via le programme F (à programmer par l'utilisateur).

Un module F-DI passivé se signale par l'état logique « 0 » à la mémoire image des entrées (MIE) de la CPU pour les canaux passivés, indépendamment des signaux effectifs des capteurs de l'installation.

Un module F-DO passivé met les canaux de sortie passivés hors courant ou tension, indépendamment des états de sortie transmis par la CPU à partir de la mémoire image des sorties (MIS).

Dépassivation

La dépassivation d'un canal ou d'un module F peut intervenir...

- automatiquement lors du redémarrage de la CPU F après une correction d'erreur (sauf en cas d'erreurs de communication)
- via le programme F (à programmer par l'utilisateur).

6.24.2. Blocs de données de la périphérie de sécurité

DB de périphérie F

- Est généré pour chaque module F lors de son insertion dans la vue des appareils
- Contient les variables d'évaluation de l'état du module
- Est alimenté avec les données du driver PROFIsafe

Utilisation des variables du DB de périphérie F

- Evaluation des valeurs du processus ou de remplacement
- Réintégration des I/Q (ACK_REI) après:
 - Des erreurs de communication PROFIsafe
 - Des erreurs sur modules F et des erreurs de canal
- Passivation manuelle, dépendant de certains états du programme de sécurité (« passivation du groupe », PASS_ON)

DB de périphérie de sécurité

Un DB de périphérie de sécurité est automatiquement créé pour chaque module de périphérie de sécurité (en mode sécurité) lors de la configuration de la périphérie de sécurité. Le DB de périphérie de sécurité contient des variables que vous pouvez évaluer dans le programme de sécurité ou encore que vous pouvez ou devez positionner. La modification directe des valeurs de départ de variables dans le DB de périphérie de sécurité n'est pas autorisée. Lors de la suppression d'une périphérie de sécurité, le DB de périphérie de sécurité correspondant est également supprimé.

Utilisation de l'accès à un DB de périphérie de sécurité

Vous accédez aux variables du DB de périphérie de sécurité :

- pour réintégrer la périphérie de sécurité après des erreurs de communication/de périphérie de sécurité/de canaux
- lorsque vous voulez passiver la périphérie de sécurité en fonction de certains états de votre programme de sécurité (par ex. passivation groupée)
- pour reparamétrer des esclaves normalisés DP de sécurité/des périphériques d'E/S normalisés
- lorsque vous voulez déterminer si des valeurs de remplacement ou de processus ont été transmises.

6.24.3. Variables des DB de périphérie

Variables en écriture par programmation
(uniquement réalisable dans le programme safety)

Name	Data type	Start value	Comment
PASS_ON	Bool	false	1=Enable passivation
ACK_NEC	Bool	true	1=Acknowledgment for reintegration required
ACK_REI	Bool	false	1=Acknowledgment for reintegration
IPAR_EN	Bool	false	Tag for parameter reassignment of fail-safe DP standard slaves/I/O standard devices or for enabling HART communication
DISABLE	Bool	false	1=Disables F-I/O
PASS_OUT	Bool	true	Passivation output
QBAD	Bool	true	1=Fail-safe values are output
ACK_BEQ	Bool	false	1=Acknowledgment requirement for reintegration
IPAR_OK	Bool	false	Tag for parameter reassignment of fail-safe DP standard slaves/I/O standard devices or for enabling HART communication
DIAG	Byte	16#0	Non-fail-safe service information
DISABLED	Bool	false	1=F-I/O disabled

Variables évaluées par programme
(possible dans le programme standard et safety)

Si le module supporte RIO for FA-Safety, le bit ACK_NEC n'a pas de signification car le comportement d'acquiescement est directement renseigné dans les paramètres du module

PASS_ON

La variable PASS_ON permet d'activer la passivation d'une périphérie de sécurité, par ex. en fonction de certains états de votre programme de sécurité. La variable PASS_ON du DB de périphérie de sécurité permet uniquement la passivation de la périphérie de sécurité complète, la passivation par canal n'est pas possible. Tant que PASS_ON = 1, la périphérie de sécurité correspondante est passivée.

ACK_NEC

Une passivation de la périphérie F concernée a lieu si la périphérie F reconnaît une erreur de périphérie. Une erreur de canal détectée est suivie, suivant le paramétrage retenu, d'une passivation du canal concerné ou de l'ensemble des canaux. La réintégration de la périphérie F concernée s'effectue en fonction de ACK_NEC :

- Avec ACK_NEC = 0 vous paramétrez une réintégration automatique.
- Avec ACK_NEC = 1 vous paramétrez une réintégration par acquiescement de l'utilisateur.

ACK_REI

Si le système F a reconnu une erreur de communication pour une périphérie F ou une erreur de périphérie alors la périphérie F concernée est passivée. La réintégration du module F ou du canal à la suite de l'élimination des erreurs est réalisée par acquiescement de l'utilisateur avec un front positif pour la variable ACK_REI de la périphérie F.

- Toujours après des erreurs de communication
- Après des erreurs de périphérie F ou de canal uniquement si paramétrage manuel de l'acquiescement avec ACK_NEC = 1

Lors de la réintégration à la suite d'une erreur de canal c'est l'ensemble des canaux dont le défaut a été supprimé qui sont réintégrés.

Un acquiescement est réalisable si la variable ACK_REQ=1

Votre programme de sécurité doit comporter un acquiescement pour chaque périphérie F via la variable ACK_REI

IPAR_EN

La variable IPAR_EN correspond à la variable iPar_EN_C du profil de bus PROFIsafe à partir de la spécification PROFIsafe V1.20. Pour savoir quand mettre à « 1 » ou à « 0 » cette variable lors d'un reparamétrage d'esclaves DP normalisés de sécurité/périphériques d'E/S normalisés, reportez-vous à la spécification PROFIsafe à partir de V1.20 ou à la documentation de l'esclave normalisé DP de sécurité/périphérique d'E/S normalisé. Notez qu'avec IPAR_EN = 1, aucune passivation de la périphérie de sécurité concernée n'est déclenchée. Si IPAR_EN = 1 doit déclencher une passivation, vous devez en plus mettre la variable PASS_ON à « 1 ».

DISABLE

La variable DISABLE permet de désactiver une périphérie F. Le maintien de DISABLE = 1 provoque la passivation de la périphérie concernée. Il n'y a alors pas d'entrée dans le tampon de diagnostic de la CPU-F pour cette périphérie F (par ex. à cause d'erreur de communication). Les entrées en déjà en attente sont qualifiées de disparaissant.

PASS_OUT

Avec l'état « 1 », le module signale qu'il s'est passivé lui-même à la suite d'une détection d'erreur. Si le module a été passivé par le programme F via la variable PASS_ON, le module laisse la variable PASS_OUT à l'état « 0 ».

QBAD

Avec l'état « 1 », le module signale qu'au moins un canal est passivé, que la passivation ait été provoquée par le module lui-même ou par le programme F via la variable PASS_ON.

ACK_REQ

Après une correction d'erreur, le module encore passivé signale avec ACK_REQ='1' qu'il est prêt pour la réintégration.

IPAR_OK

La variable IPAR_OK correspond à la variable iPar_OK_S du profil de bus PROFIsafe à partir de la spécification PROFIsafe V1.20. Pour savoir comment évaluer cette variable lors d'un reparamétrage d'esclaves DP normalisés de sécurité/périphériques d'E/S normalisés, reportez-vous à la spécification PROFIsafe à partir de V1.20 ou à la documentation de l'esclave DP normalisé de sécurité ou du périphérique d'E/S normalisé.

DIAG

La variable DIAG met à disposition, à des fins de maintenance, une information non sécurisée (1 octet) sur les erreurs survenues. Vous pouvez lire cette information via des systèmes de contrôle-commande ou l'évaluer dans votre programme utilisateur standard. Les bits DIAG restent mémorisés jusqu'à l'acquiescement de la variable ACK_REI ou jusqu'à une réintégration automatique. Dans le programme de sécurité, vous pouvez affecter cette variable à une variable standard via l'instruction MOVE.

État de la valeur des CPU 1200/1500F

Etat de la valeur

- Information complémentaire au sujet de la valeur d'un canal de périphérie F.
- Est pris en charge par les modules ET 200SP, ET 200S, ET 200iSP, ET 200pro, ET 200M et ET 200MP.
- L'état de la valeur renseigne la validité de la valeur du canal correspondant:
 - 1: une **valeur de processus valide** est émise pour le canal.
 - 0: une **valeur de substitution** est émise pour le canal.
- L'accès à la valeur du canal et à l'état de la valeur d'une périphérie F est uniquement autorisé à partir d'un seul groupe d'exécution F.
- L'état de la valeur **est consigné dans la mémoire image des entrées (MIE)**.

État de la valeur

L'état de la valeur est une information binaire supplémentaire sur une valeur de canal d'une périphérie de sécurité. Il est consigné dans la mémoire image des entrées (MIE).

L'état de la valeur est pris en charge par les modules de sécurité S7-1500/ET 200MP, ET 200SP, ET 200S, ET 200iSP, ET 200pro, S7-1200 ou F-SM S7-300, les périphériques d'E/S normalisés de sécurité et les esclaves DP normalisés de sécurité qui gèrent le profil « RIOforFA-Safety ».

Nous vous recommandons, pour l'état de la valeur, de compléter le nom de la valeur du canal avec « _VS », par ex. "STOP_1_VS".

L'état de la valeur renseigne sur la validité de la valeur du canal correspondant :

- 1 : une valeur de processus valide est émise pour le canal
- 0 : une valeur de remplacement est émise pour le canal

L'accès à la valeur de canal et à l'état de la valeur d'une périphérie de sécurité n'est autorisé qu'à partir d'un même groupe d'exécution

6.24.4. Bits d'état de la valeur pour F-DI

Octet dans la CPU F	Bits occupés dans la CPU F, par module F :							
	7	6	5	4	3	2	1	0
x + 0	DI ₇	DI ₆	DI ₅	DI ₄	DI ₃	DI ₂	DI ₁	DI ₀
x + 1	Etat de la valeur pour DI ₇	Etat de la valeur pour DI ₆	Etat de la valeur pour DI ₅	Etat de la valeur pour DI ₄	Etat de la valeur pour DI ₃	Etat de la valeur pour DI ₂	Etat de la valeur pour DI ₁	Etat de la valeur pour DI ₀

x = adresse de début du module

Occupation des adresses MIE

• Les bits d'état de la valeur suivent directement les valeurs de canal dans la MIE.

F-DI 8x24VDC HF_3 [F-DI 8x24VDC HF]				
Général	Variable IO	Constantes système	Textes	
Nom	Type	Adresse	Table de variables	
F-DI Entree 0	Bool	%I0.0	Table variables standard	
F-DI Entree 1	Bool	%I0.1	Table variables standard	
F-DI Entree 2	Bool	%I0.2	Table variables standard	
F-DI Entree 3	Bool	%I0.3	Table variables standard	
F-DI Entree 4	Bool	%I0.4	Table variables standard	
F-DI Entree 5	Bool	%I0.5	Table variables standard	
F-DI Entree 6	Bool	%I0.6	Table variables standard	
F-DI Entree 7	Bool	%I0.7	Table variables standard	
Etat Valeur F-DI pour entree 0	Bool	%I1.0	Table variables standard	
Etat Valeur F-DI pour entree 1	Bool	%I1.1	Table variables standard	
Etat Valeur F-DI pour entree 2	Bool	%I1.2	Table variables standard	
Etat Valeur F-DI pour entree 3	Bool	%I1.3	Table variables standard	
Etat Valeur F-DI pour entree 4	Bool	%I1.4	Table variables standard	
Etat Valeur F-DI pour entree 5	Bool	%I1.5	Table variables standard	
Etat Valeur F-DI pour entree 6	Bool	%I1.6	Table variables standard	
Etat Valeur F-DI pour entree 7	Bool	%I1.7	Table variables standard	

État de la valeur pour les modules d'entrée et sortie TOR

L'état de la valeur est influencé par la détection de rupture de fil, les courts-circuits, la surveillance de gigue (flottement), la prolongation des impulsions et le contrôle de plausibilité.

Remarque

Vous ne pouvez accéder qu'aux adresses occupées par les données utiles et l'état de la valeur. Les autres adresses utilisées par les modules F sont notamment réservées à la communication de sécurité entre les modules F et la CPU F conformément à PROFIsafe. En cas d'évaluation 1oo2 (1de2) des capteurs, les deux canaux sont regroupés. En cas d'évaluation 1oo2 (1de2) des capteurs, vous ne devez accéder qu'au canal de poids faible dans le programme de sécurité.

6.24.5. Bits d'état de la valeur pour F-DQ

Octet dans la CPU F	Bits occupés dans la CPU F, par module F :							
	7	6	5	4	3	2	1	0
x + 0	—	—	—	—	Etat de la valeur pour DQ ₃	Etat de la valeur pour DQ ₂	Etat de la valeur pour DQ ₁	Etat de la valeur pour DQ ₀

x = adresse de début du module

Occupation des adresses MIE

Octet dans la CPU F	Bits occupés dans la CPU F, par module F :							
	7	6	5	4	3	2	1	0
x + 0	—	—	—	—	DQ ₃	DQ ₂	DQ ₁	DQ ₀

x = adresse de début du module

Occupation des adresses MIS

- Les bits d'état de la valeur sont reportés dans la MIE avec la même structure que les valeurs du canal dans la MIS.

Général				Variable IO	Constantes système	Textes
Nom	Type	Adresse	Table de variables			
F-DO Sortie 0	Bool	%Q43.0	Table variables standard			
F-DO Sortie 1	Bool	%Q43.1	Table variables standard			
F-DO Sortie 2	Bool	%Q43.2	Table variables standard			
F-DO Sortie 3	Bool	%Q43.3	Table variables standard			
Etat valeur F-DO Sortie 0	Bool	%I43.0	Table variables standard			
Etat valeur F-DO Sortie 1	Bool	%I43.1	Table variables standard			
Etat valeur F-DO Sortie 2	Bool	%I43.2	Table variables standard			
Etat valeur F-DO Sortie 3	Bool	%I43.3	Table variables standard			

6.24.6. Bits d'état de la valeur pour F-PM

Octet dans la CPU F	Bits occupés dans la CPU F, par module F :							
	7	6	5	4	3	2	1	0
x + 0	—	—	—	—	—	—	DI ₁	DI ₀
x + 1	—	—	—	—	—	—	Etat de la valeur pour DI ₁	Etat de la valeur pour DI ₀
x + 2	—	—	—	—	—	—	—	Etat de la valeur pour DQ ₀

Occupation des adresses MIE

Octet dans la CPU F	Bits occupés dans la CPU F, par module F :							
	7	6	5	4	3	2	1	0
x + 0	—	—	—	—	—	—	—	DQ ₀

Occupation d'adresse MIS

x = adresse de début du module

Propriétés				
Général	Variable IO	Constantes système	Textes	
Nom	Type	Adresse	Table de variables	Co
F-PM Entrée 0	Bool	%I36.0	Table variables standard	
F-PM Entrée 1	Bool	%I36.1	Table variables standard	
F-PM Sortie 0	Bool	%Q36.0	Table variables standard	
Etat valeur F-PM Entrée 0	Bool	%I37.0	Table variables standard	
Etat valeur F-PM Entrée 1	Bool	%I37.1	Table variables standard	
Etat valeur F-PM Sortie 0	Bool	%I38.0	Table variables standard	

6.24.7. Bits d'état de la valeur pour F-AI

Byte in the F-CPU	Assigned bytes/bits in the F-CPU per F-I/O:							
	7	6	5	4	3	2	1	0
x + 0	Channel value AI ₀							
...	...							
x + 10	Channel value AI ₅							
x + 12	—	—	Value	Value	Value	Value	Value	Value

x = adresse de début du module

Occupation des adresses MIE

F-AI 6x0/4...20mA HART_1 [F-AI 6x0/4...20mA HART]				
General	IO tags	System constants	Texts	
Name	Type	Address	Tag table	
F-DI Input 0	Int	%IW54	Default tag table	
F-DI Input 1	Int	%IW56	Default tag table	
F-DI Input 2	Int	%IW58	Default tag table	
F-DI Input 3	Int	%IW60	Default tag table	
F-DI Input 4	Int	%IW62	Default tag table	
F-DI Input 5	Int	%IW64	Default tag table	
Value status F-DI Input 0	Bool	%I66.0	Default tag table	
Value status F-DI Input 1	Bool	%I66.1	Default tag table	
Value status F-DI Input 2	Bool	%I66.2	Default tag table	
Value status F-DI Input 3	Bool	%I66.3	Default tag table	
Value status F-DI Input 4	Bool	%I66.4	Default tag table	
Value status F-DI Input 5	Bool	%I66.5	Default tag table	

6.25. Exercice 3 : Comprendre l'état de la valeur

La table de visualisation peut être copiée à partir de la bibliothèque.

	Adresse	Format d'affichage	Valeur visualisation	Valeur de forçage
1	"eStop1"	%I4.1	BOOL	FALSE
2	"eStop1VS"	%I5.1	BOOL	FALSE
3	"eStop2"	%I4.3	BOOL	FALSE
4	"eStop2VS"	%I5.3	BOOL	FALSE
5	"eStop3"	%I10.0	BOOL	FALSE
6	"eStop3VS"	%I11.0	BOOL	FALSE
7	"eStop4"	%I22.0	BOOL	FALSE
8	"eStop4VS"	%I23.0	BOOL	FALSE
9	"motor1"	%Q17.0	BOOL	FALSE
10	"motor1VS"	%I17.0	BOOL	FALSE
11	"motor2"	%Q17.1	BOOL	FALSE
12	"motor2VS"	%I17.1	BOOL	FALSE
13	"autoSwitch"	%I4.0	BOOL	FALSE
14	"autoSwitchVS"	%I5.0	BOOL	FALSE
15	"serviceSwitch"	%I4.4	BOOL	FALSE
16	"serviceSwitchVS"	%I5.4	BOOL	FALSE
17	"twoHandS1"	%I22.2	BOOL	FALSE
18	"twoHandS1VS"	%I23.2	BOOL	FALSE
19	"twoHandS2"	%I22.6	BOOL	FALSE
20	"twoHandS2VS"	%I23.6	BOOL	FALSE
21	"sensorRfid1"	%I22.1	BOOL	FALSE
22	"sensorRfid1VS"	%I23.1	BOOL	FALSE
23	"sensorRfid2"	%I22.5	BOOL	FALSE
24	"sensorRfid2VS"	%I23.5	BOOL	FALSE

Pourquoi chaque état de signal et état de valeur sont-ils à 0 ?

Énoncé

On veut à présent vérifier le comportement de l'état de la valeur d'un canal d'entrée/sortie de la station de travail.

Procédure

1. Copiez par glisser-déposer la table de variables « ValueStatusFio » et la table de visualisation « Vérification Valeur d'état » de la bibliothèque dans votre projet
2. Observez l'état de la valeur et le signal de process des différents canaux lorsque vous déclenchez différents capteurs (E1, E2, RFID, etc.)
3. Analysez pourquoi tous les canaux sont actuellement passivés (état de la valeur = 0)

Solution

Explication :



.....

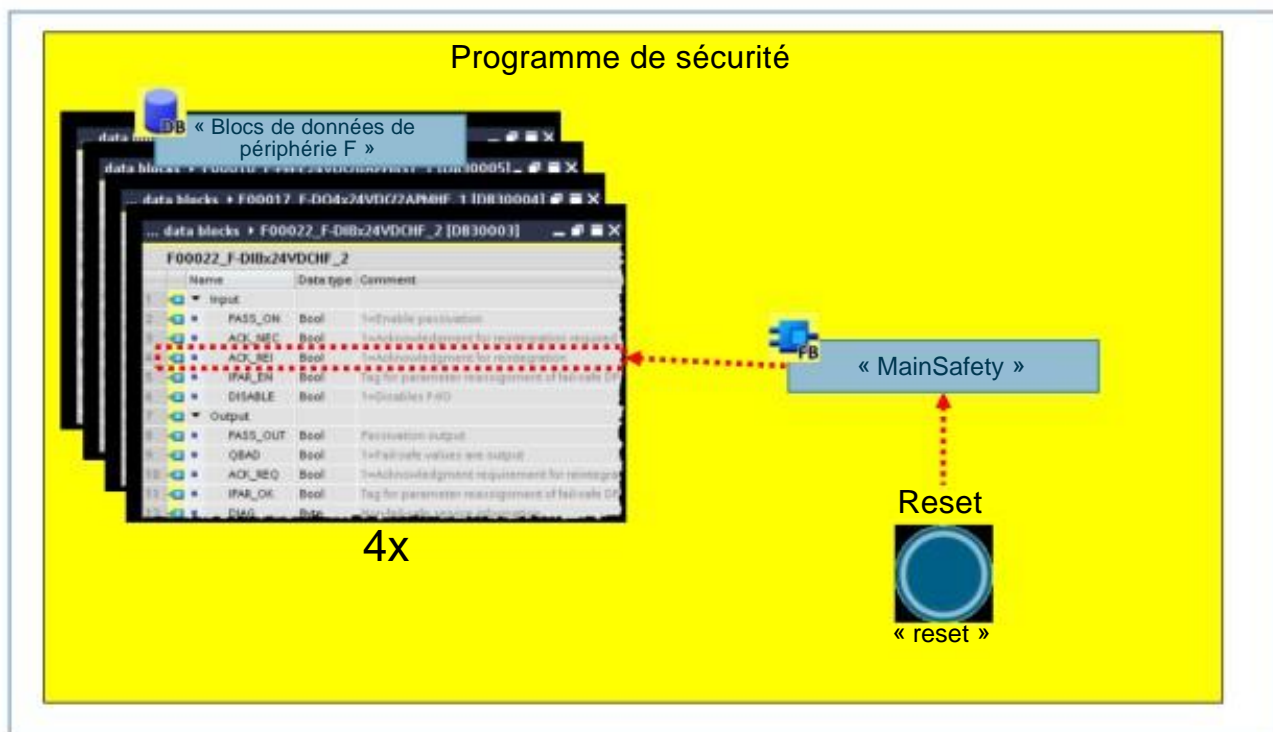
.....

.....

.....

.....

6.26. Exercice 4 : Réintégration de la périphérie F



Énoncé

L'utilisateur doit pouvoir réintégrer une périphérie F passivée à l'aide d'un bouton d'acquiescement « reset ».

REMARQUE : pour cet exercice, n'utilisez pas le bloc « ACK-GL » de la bibliothèque Safety. À titre d'illustration, l'acquiescement doit être ici directement déclenché via les DB de périphérie.

Procédure

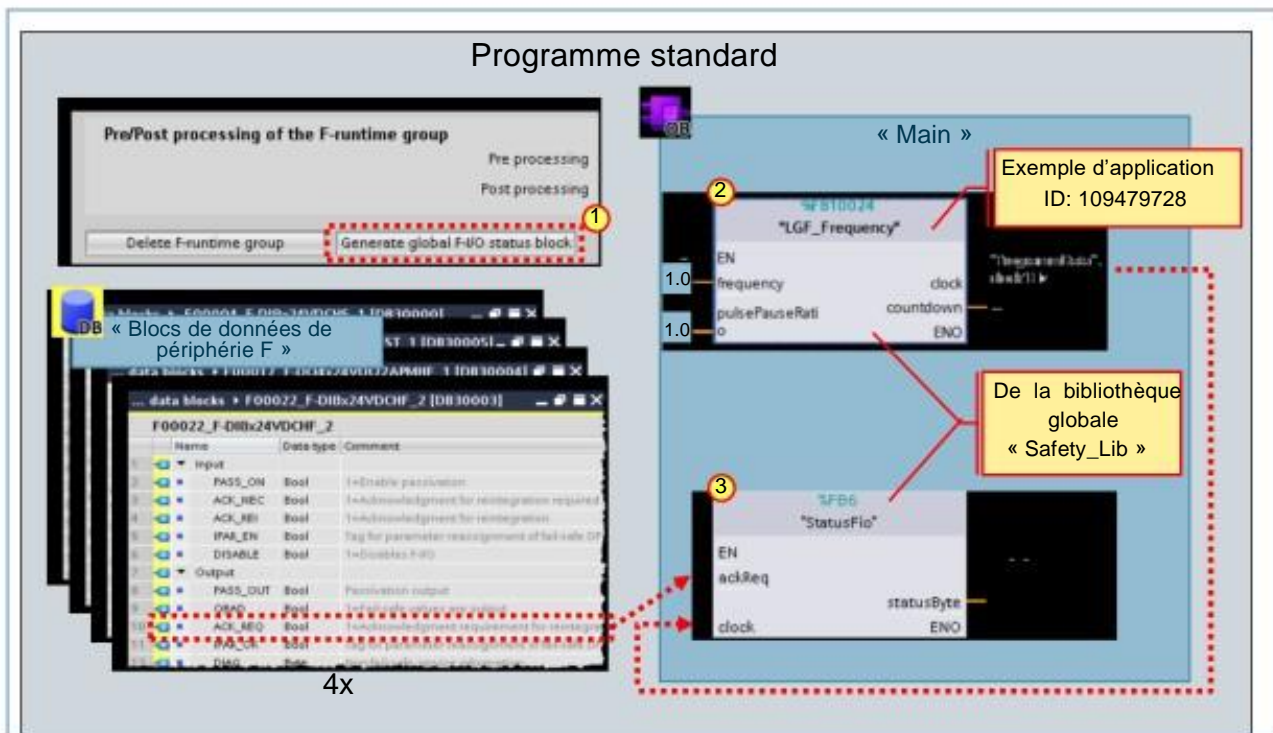
1. Programmez la réintégration directement dans le bloc « MainSafety ». Affectez le bouton d'acquiescement « reset » à chaque entrée (ACK_REI) de la périphérie F
2. Enregistrez votre projet et chargez les modifications dans la CPU.

Résultat

Testez la fonctionnalité en provoquant une erreur de canal via l'interrupteur de court-circuit. Après la suppression du court-circuit, la carte doit se laisser réintégrer avec le bouton d'acquiescement (Reset).

Interfaces concernées		
Entrées	Standard	Sécurité
	"reset"	-
Blocs de données	Global	Système
	-	F-I/O DB.ACK_REI

6.27. Exercice 5 : Evaluation de l'état de la périphérie F



Enoncé

Actuellement, l'utilisateur est informé de l'état de la périphérie F par le diagnostic système intégré à l'IHM. Le diagnostic doit à présent être complété par un affichage avec LED :

- Dès qu'un module de périphérie F est passivé, il faut activer les « Top-Lights » rouges ("deviceLeds".redTopLight) du banc de formation.
- Dès qu'un module de périphérie F demande une réintégration, il faut faire clignoter les « Top-Lights » rouges ("deviceLeds".redTopLight) (1Hz) de même que la LED du bouton d'acquiescement ("deviceLeds".resetLed) (1Hz)

Remarque : Le cours se base sur la programmation du programme de sécurité. L'évaluation et le pilotage des LED sont déjà préprogrammés et disponibles dans la bibliothèque "Safety_Bibfr". Les données nécessaires ne sont plus qu'à transférer.

Procédure

1. Afin d'évaluer l'état de l'ensemble de la périphérie F, créez un « bloc d'état global de la périphérie F » pour votre groupe d'exécution « Safety Administration -> F-runtime group »

Remarque : Le bloc ne doit pas être appelé. Il sera appelé automatiquement et traité ultérieurement par le bloc « StatusFio ».

2. Programmez une fréquence de 1Hz et enregistrez la dans un bloc de données global "ProgrammData"clock1Hz. Utilisez le bloc « LGF_Frequency » de la bibliothèque « Safety_Lib->Exercice_5 » et appelez le dans le programme standard.
3. Pour exploiter l'état de la périphérie F utilisez le bloc préprogrammé « StatusFio » de la bibliothèque « Safety_Libfr->Exercice_5 ». Appelez le bloc dans le programme standard principal « Main » et affectez les entrées à l'aide des données nécessaires (cf. vue). Rassembler les requêtes d'acquiescement (ACK REQ) issues des DB de périphérie F.

Enregistrez votre projet et chargez toutes les modifications dans la CPU

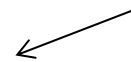
Résultat

Testez les fonctionnalités comme demandées dans le cahier des charges.

Interfaces concernées		
Blocs de données	Global	Système
	"ProgrammData".clock1Hz	"F-I/O DB".ACK_REQ

Remarque

Il faut évaluer l'ensemble des quatre blocs d'état de la périphérie F.



6.28. Exercice 6 : Encore un test pour comprendre l'état de la valeur

1513F [CPU 1513F-1 PN] ▶ Tables de visualisation et de forçage permanent ▶ État

	Nom	Adresse	Format d'affichage	Valeur visualisation	Valeur de forçage
1	"eStop1"	%I4.1	BOOL	<input type="checkbox"/> FALSE	
2	"eStop1VS"	%I5.1	BOOL	<input checked="" type="checkbox"/> TRUE	
3	"eStop2"	%I4.3	BOOL	<input checked="" type="checkbox"/> TRUE	
4	"eStop2VS"	%I5.3	BOOL	<input checked="" type="checkbox"/> TRUE	
5	"eStop3"	%I10.0	BOOL	<input checked="" type="checkbox"/> TRUE	
6	"eStop3VS"	%I11.0	BOOL	<input checked="" type="checkbox"/> TRUE	
7	"eStop4"	%I22.0	BOOL	<input checked="" type="checkbox"/> TRUE	
8	"eStop4VS"	%I23.0	BOOL	<input checked="" type="checkbox"/> TRUE	
9	"motor1"	%Q17.0	BOOL	<input type="checkbox"/> FALSE	
			BOOL	<input checked="" type="checkbox"/> TRUE	
			BOOL	<input type="checkbox"/> FALSE	
			BOOL	<input checked="" type="checkbox"/> TRUE	
			BOOL	<input type="checkbox"/> FALSE	
			BOOL	<input checked="" type="checkbox"/> TRUE	
15	"serviceSwitch"	%I4.4	BOOL	<input type="checkbox"/> FALSE	
16	"serviceSwitchVS"	%I5.4	BOOL	<input checked="" type="checkbox"/> TRUE	
17	"twoHandS1"	%I22.2	BOOL	<input type="checkbox"/> FALSE	
18	"twoHandS1VS"	%I23.2	BOOL	<input checked="" type="checkbox"/> TRUE	
19	"twoHandS2"	%I22.6	BOOL	<input type="checkbox"/> FALSE	
20	"twoHandS2VS"	%I23.6	BOOL	<input checked="" type="checkbox"/> TRUE	
21	"sensorRfid1"	%I22.1	BOOL	<input type="checkbox"/> FALSE	
22	"sensorRfid1VS"	%I23.1	BOOL	<input checked="" type="checkbox"/> TRUE	
23	"sensorRfid2"	%I22.5	BOOL	<input type="checkbox"/> FALSE	
24	"sensorRfid2VS"	%I23.5	BOOL	<input checked="" type="checkbox"/> TRUE	

État de la valeur après déclenchement du court-circuit (coupure par canal) pour l'arrêt d'urgence 1

Énoncé

On veut vérifier une nouvelle fois le comportement de l'état de la valeur d'un canal de périphérie F (cf. exercice 3).

Procédure

1. Observez la réaction des variables concernées lorsque :
 - un dispositif de protection est déclenché (arrêt d'urgence, porte de protection, etc.)
 - vous actionnez le commutateur de court-circuit (« Short circuit ») sur la station de travail

Résultat

Tous les modules F sont à présent utilisés dans le programme de sécurité (via l'exercice 4) et sont dépassivés après le démarrage de la CPU et délivrent des valeurs de process valides.

6.28.1. Exercice 6 : Test du câblage des entrées et sorties de sécurité

...7-1513F [CPU 1513F-1 PN] ▶ Tables de visualisation et de forçage permanent ▶ Vérification

	Nom	Adresse	Format d'affichage	Valeur visualisatio	Valeur de forçage
1	"eStop1"	%I4.1	BOOL	FALSE	
2	"eStop2"	%I4.3	BOOL	TRUE	
3	"eStop3"	%I10.0	BOOL	TRUE	
4	"eStop4"	%I22.0	BOOL	TRUE	
5	"motor1"	%Q17.0	BOOL	FALSE	TRUE
6	"motor2"	%Q17.1	BOOL	FALSE	TRUE
7	"powerValves"	%Q10.0	BOOL	FALSE	TRUE
8	"autoSwitch"	%I4.0	BOOL	FALSE	
9	"serviceSwitch"	%I4.4	BOOL	FALSE	
10	"twoHandS1"	%I22.2	BOOL	FALSE	
11	"twoHandS2"	%I22.6	BOOL	FALSE	
12	"sensorRfid1"	%I22.1	BOOL	FALSE	
13	"sensorRfid2"	%I22.5	BOOL	FALSE	
14	"start"	%I2.0	BOOL	FALSE	
15	"reset"	%I2.3	BOOL	FALSE	
16	"resetLed"	%Q2.7	BOOL	FALSE	
17	"valve1"	%Q3.0	BOOL	FALSE	FALSE
18	"valve2"	%Q3.1	BOOL	FALSE	FALSE
19	<Ajouter>				

Forçage des sorties
(uniquement possible avec mode de sécurité désactivé sur la CPU)

Énoncé

On veut à présent vérifier le câblage de toutes les entrées et sorties de la station de travail.

Procédure

1. Copiez par glisser-déposer la table de visualisation « Contrôle du câblage » de la bibliothèque dans votre projet
2. Vérifiez le câblage des entrées en actionnant les éléments de commande correspondants sur la maquette de test et comparez avec les valeurs de visualisation affichées.
3. Vérifiez le câblage des sorties de sécurité en entrant les valeurs de forçage sur la PG et en comparant avec les réactions des actionneurs de la maquette de formation.
 - Acquitez le message « Mode de sécurité actif »
 - Entrez ensuite votre mot de passe CPU
 - Confirmez que vous voulez bien désactiver le mode de sécurité

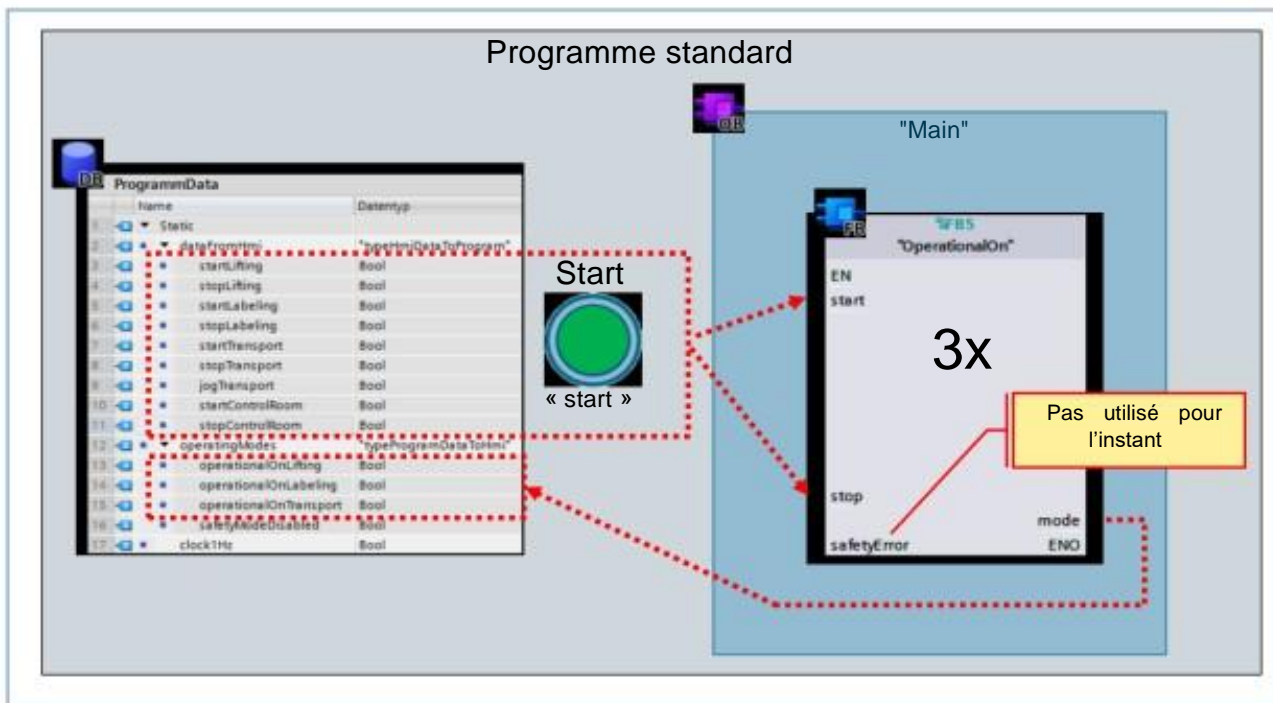
Résultat

Toutes les entrées et sorties de la station de travail devraient être correctement raccordées. Dans le cas contraire, vérifiez le paramétrage des canaux concernés ainsi que l'affectation à la mémoire image.

Attention !

Ne modifiez pas le câblage existant. Si vous pensez qu'il y a une erreur de câblage, parlez-en au formateur.

6.29. Exercice 7 : programmer les modes de fonctionnement



Enoncé

La machine « Etiqueteuse » doit être considérée comme une installation indépendante et autonome. Il s'agit de programmer trois parties indépendantes de l'installation disposant chacune de leurs modes de fonctionnement :

Dispositif de levage :

- Automatique
- Arrêt

Etiqueteuse :

- Automatique
- Arrêt

Transport :

- Automatique
- Arrêt

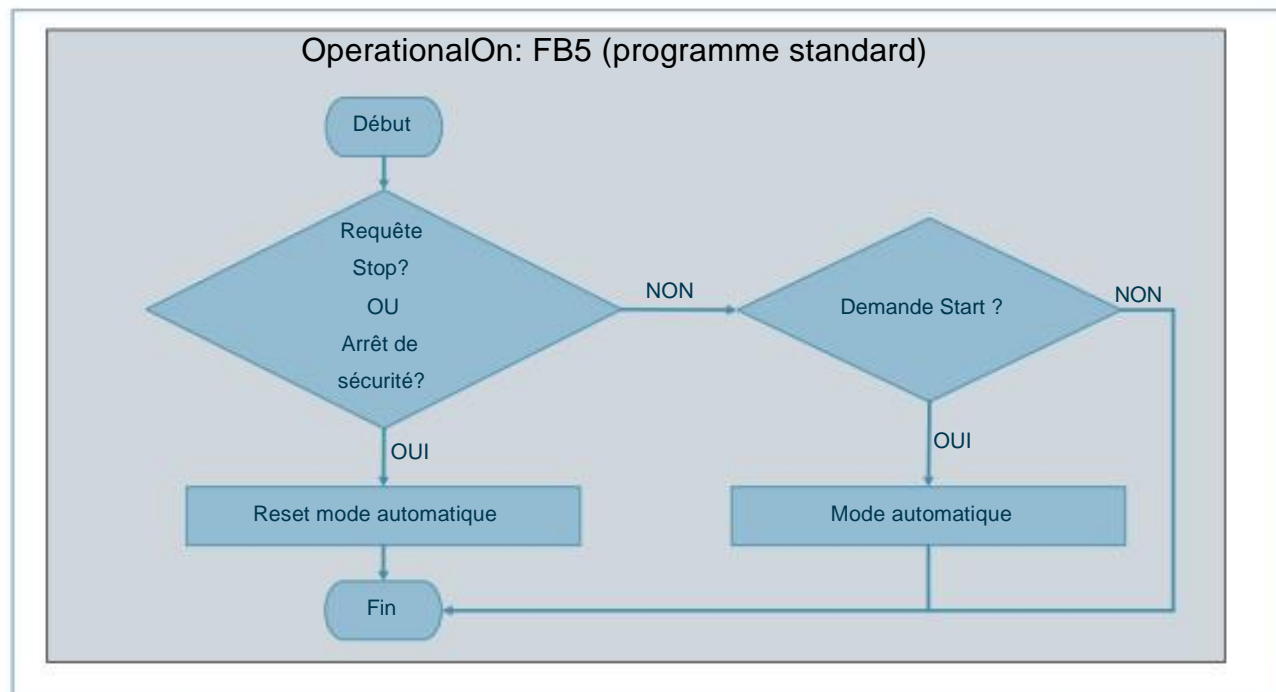
Les modes de fonctionnement doivent être pilotés séparément via l'IHM ou simultanément via le poste de commande (IHM et bouton de démarrage). Le programme de sécurité devra ultérieurement avoir la possibilité de réinitialiser les modes de fonctionnement (safetyError).

Procédure

1. Copiez le bloc préprogrammé « OperationalOn » de la bibliothèque « Safety_Bibfr->Exercice_7 » dans le répertoire des blocs standards et familiarisez-vous avec la fonctionnalité.
2. Bloc de fonction Mode de fonctionnement (Description générale)
Générez les modes de fonctionnement nécessaires via le bloc « OperationalOn » dans votre programme utilisateur standard. Enregistrez tous les modes de fonctionnement au niveau du bloc de données global « ProgrammData » (Cf. vue). L'entrée « safetyError » reste encore non affectée.

Une description détaillée de l'exercice se trouve en page suivante.

6.29.1. Exercice 7 : Organigramme



1. Bloc de fonction Mode de fonctionnement (Description détaillée)

Insérez trois nouveaux réseaux dans le programme standard « Main » pour y appeler le bloc « OperationalOn » avec sa propre instance pour chaque partie de l'installation. Les modes de fonctionnement individuels de chaque partie de l'installation sont gérés par ces appels. Les modes automatique (Auto) sont pilotés par les signaux suivants :

- Bouton démarrage (« démarrage »)
- Démarrage IHM d'une partie de l'installation ("ProgrammData".dataFromHmi.startXXXXX)
- Démarrage IHM du poste de contrôle ("ProgrammData".dataFromHmi.startControlRoom)

Les modes de fonctionnement automatique sont désélectionnés par les signaux suivants : – Arrêt partiel de l'installation IHM ("ProgrammData".dataFromHmi.stopXXXXX)

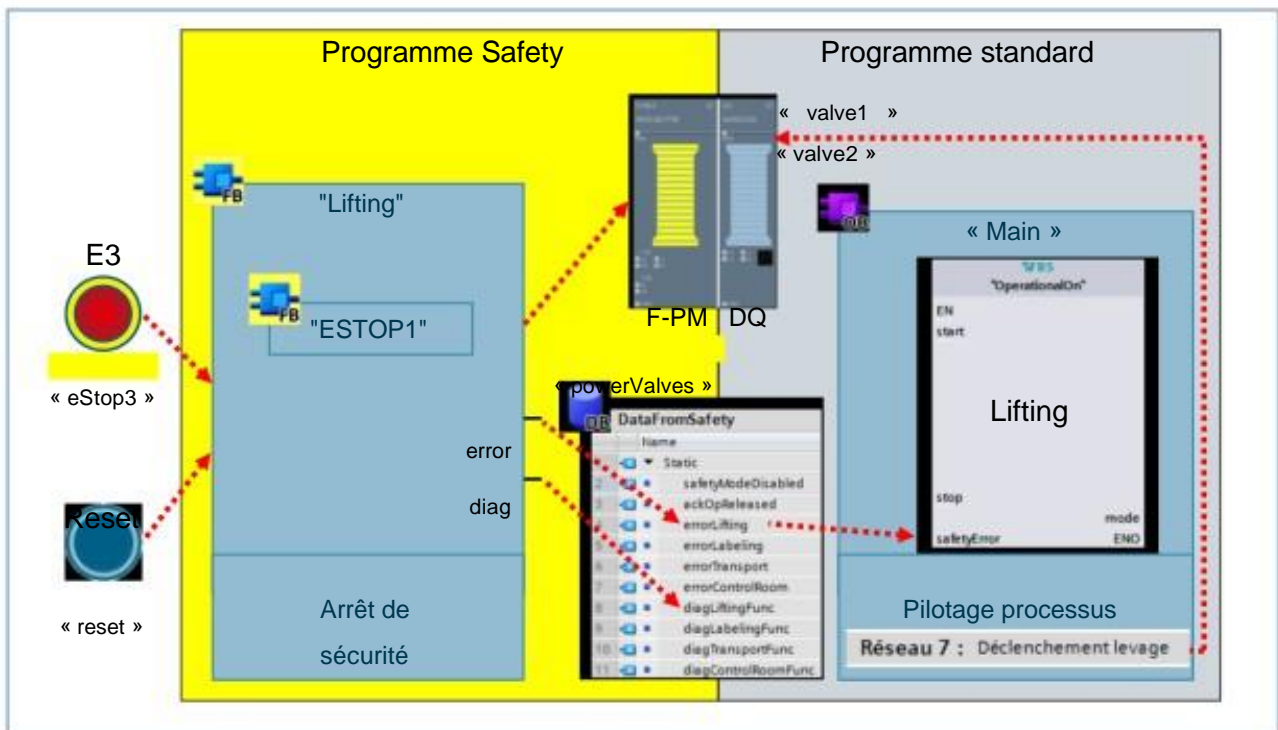
– Arrêt IHM du poste de commande ("ProgrammData".dataFromHmi.stopControlRoom) Les modes de fonctionnement actuels (mode) doivent être mémorisés individuellement dans le bloc de données globales "ProgrammData".operatingModes.

L'entrée « safetyError » n'est pas encore affectée. L'entrée sera affectée dans les exercices suivants.

2. Chargez toutes les modifications dans la CPU.
3. Enregistrez le projet et testez la fonctionnalité.

Interfaces concernées		
Entrées	Standard	Sécurité
	"start"	-
Blocs de données	Global	Système
	"ProgrammData".dataFromHmi	-
	"ProgrammData".operatingModes	-

6.30. Exercice 8: Dispositif de levage



Enoncé

La partie d'installation « système de levage » permet d'acheminer les pièces vers l'étiqueteuse. Nous ne considérons ici que la fonctionnalité des vannes d'arrêt de sécurité. Les fonctions de descente et de montée du dispositif ne sont pas traitées dans cet exercice.

Les vannes d'arrêt doivent être commutées en fonctionnement normal. En mode automatique, les vannes doivent être commutables et bloquées en cas d'arrêt. Une coupure de sécurité doit être réalisée via un dispositif d'arrêt d'urgence. Le programme de sécurité doit bloquer le pilotage en fonctionnement normal des vannes par coupure de l'alimentation en énergie. Après le déclenchement de l'arrêt d'urgence, l'alimentation en énergie ne doit être validée qu'après un acquittement. Le mode automatique doit être désactivé en cas de déclenchement de l'arrêt d'urgence.

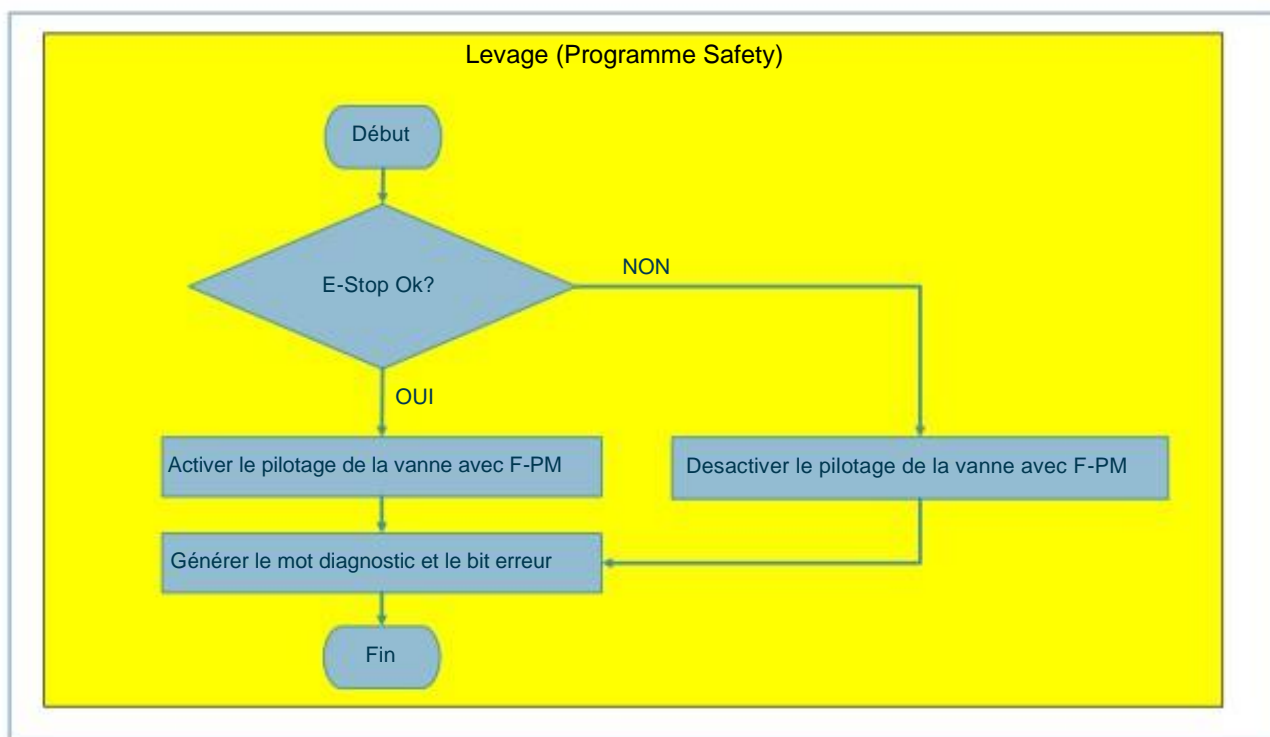
Remarque : Lors de la programmation tenez compte des principaux aspects du guide de programmation comme la réutilisabilité et la structure du programme.

Procédure

1. Le programme standard « Main » doit, après évaluation de l'ensemble des modes de fonctionnement, piloter les deux vannes « vanne1 » et « vanne2 » lorsque le dispositif de levage se trouve en automatique : "ProgrammData".operatingModes.operationalOnLifting .
2. Bloc de programme « Levage » (Description générale)
Réalisez le bloc de sécurité « Levage » et programmez la fonctionnalité demandée (Enoncé). Utilisez la fonction de sécurité « ESTOP1 » de la liste des instructions pour la réalisation de l'arrêt d'urgence. L'acquiescement de la fonction de sécurité à lieu via le bouton d'acquiescement du banc de formation. Implémentez également le diagnostic comme décrit dans l'étape 3 et transférez les données aux blocs de données correspondants (Cf. vue).

Une description de l'exercice est détaillée à la page suivante.

6.30.1. Exercice 8: Organigramme



1. Bloc de fonction « Levage » (Description détaillée)

Le bloc doit surveiller la coupure d'urgence E3 via la fonction de sécurité « ESTOP ». Dès que l'arrêt d'urgence E3 est appuyé (« S-E3 ») =0, l'alimentation du groupe de potentiel doit immédiatement être coupée par le module de sécurité (« PowerValves » =0).

Les modules standard DQ intégrés au même groupe de potentiel (branché aux vannes) sont ainsi coupés en sécurité.

Après le déverrouillage de l'arrêt d'urgence E3 (« S-E3 » =1) et l'activation de la touche d'acquiescement (« S-Reset » =1) il faut rétablir la tension d'alimentation (« PowerValves » =1).

Interfaces concernées		
Entrées	Standard	Sécurité
	« reset » (I2.3)	« eStop3 » (I10.0)
Sorties	Standard	Sécurité
		« PowerValves »
Blocs de données	Global	Système
	"DataFromSafety".errorLifting	
	"DataFromSafety".diagLiftingFunc	

La suite à la page suivante

6.30.2. Exercice 8 : Diagnostic dans le programme safety

Diagnostics standardisés

Chaque boucle de sécurité doit générer un diagnostic homogène utilisable dans le programme utilisateur standard et l'IHM:

- Mot de diagnostic
- Bit d'erreur (déclenchement ou erreur d'une fonction safety)

Structure du mot de diagnostic:

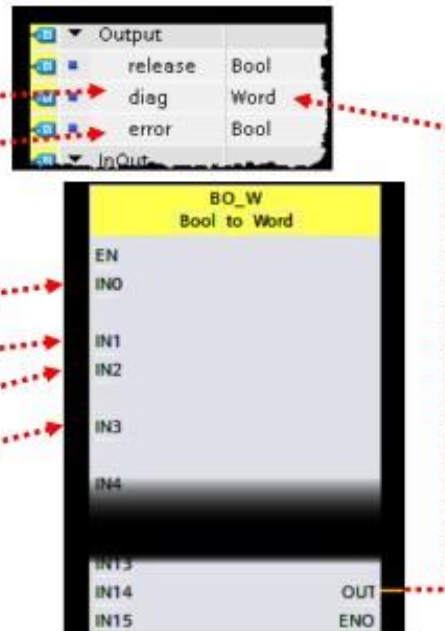
Fonction Safety 1 (2 bits):

- Bit 0: OK
- Bit 1: requête d'acquiescement

Fonction Safety 2 (2 bits):

- Bit 2: OK
- Bit 3: requête d'acquiescement

etc.



SITRAIN © Siemens SAS 2020
Page 82

TIA-SAFETY
Programmation

2. Diagnostic dans le bloc « Lifting »

Principe du diagnostic

Afin de réduire les temps d'arrêt d'une installation à un minimum il est indispensable de disposer d'un diagnostic cohérent, compréhensible et clair. Une évaluation du diagnostic tout comme la visualisation ne représentent pas une partie principale de la sécurité du site c'est pour cette raison que le diagnostic est déjà, pour sa grosse partie, intégrée (IHM et CPU.)

Que faut-il encore programmer ?

Ce qui manque encore c'est une mise en place d'un diagnostic homogène des fonctions de sécurité pour le programme de sécurité.

Afin de faire fonctionner le diagnostic et la visualisation existants, il faut que chaque partie du site comprenant des fonctions de sécurité actives retournent un diagnostic homogène au programme utilisateur standard.

Structure des remontées de diagnostic des parties de l'installation (blocs de fonctions du programme de sécurité):

- Mot de diagnostic « diag » (Word)

L'état de chaque fonction de sécurité est stocké dans le mot de diagnostic. Deux bits sont réservés pour chaque fonction de sécurité :

Bit 0 : la fonction de sécurité est OK (1)

Bit 1 : Requête d'acquiescement (1)

L'ordre des fonctions de sécurité dans le mot de diagnostic est à extraire de l'IHM.

- Bit d'erreur « error » (Bool)

Le bit erreur est positionné dès qu'une fonction de sécurité de ce bloc est activée (ESTOP1 et SFDDOR) ou remonte une erreur (FDBACK).



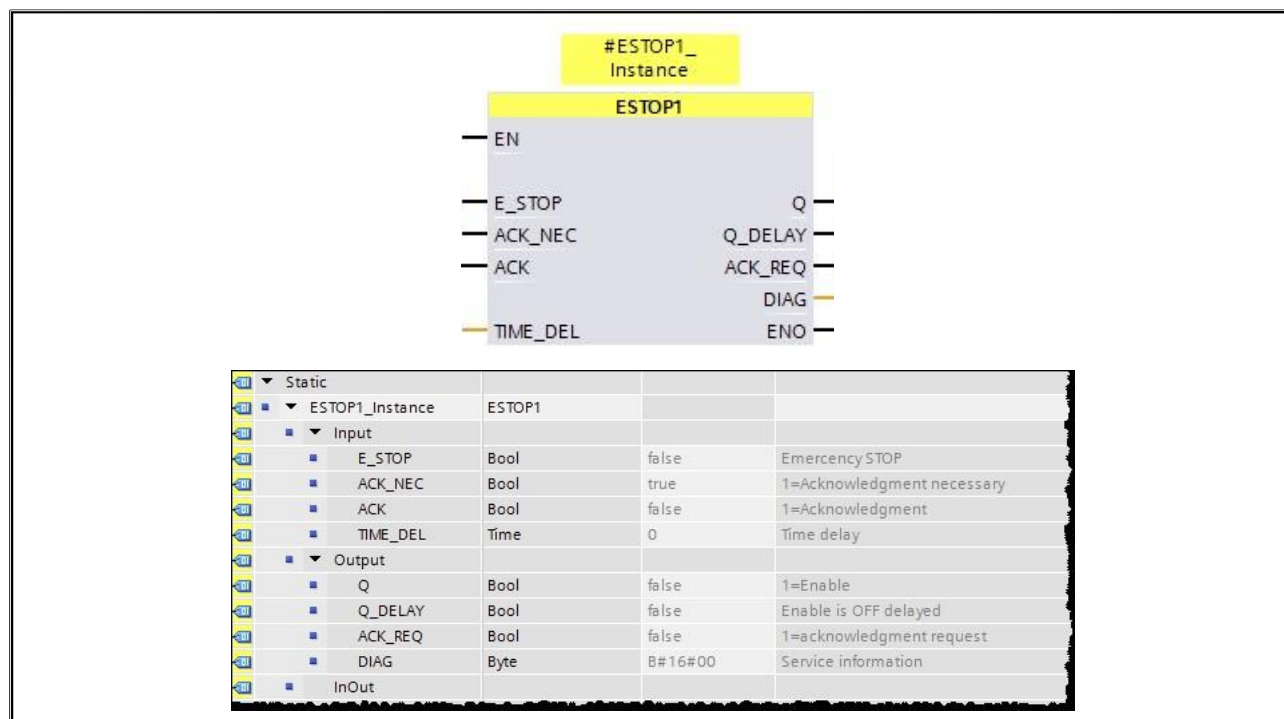
Bit 0,1 ← Arrêt Urgence: ● Déclenché
Bit 2,3 ← Porte sécurité: ● Verrouillé
Bit 4,5 ← Feedback: ● OK



Par ex. Transport :3 fonctions de sécurité

3. Enregistrez les données de diagnostic dans le bloc de données « DataFromSafety ».
"DataFromSafety".errorLifting
"DataFromSafety".diagLiftingFunc
4. Une coupure de sécurité (« DataFromSafety ».errorLifting) doit également désactiver le mode automatique du module de levage. Affectez le signal de coupure (errorLifting) à l'entrée « SafetyError » du bloc « OperationalOn » (module de levage).
5. Enregistrez le projet et testez la fonctionnalité

6.30.3. Fonction de sécurité ESTOP1



Cette instruction réalise un arrrt/coupure d'urgence avec acquittement pour les catégories d'arrt 0 et 1.

Le signal de validation Q est remis à 0 dès que l'entrée E_STOP prend l'état de signal 0 (catégorie d'arrt 0). Le signal de validation Q_DELAY est remis à 0 après écoulement du temps de retard paramétré à l'entrée TIME_DEL (catégorie d'arrt 1).

Le signal de validation Q n'est remis à 1 que lorsque l'entrée E_STOP prend l'état de signal 1 et qu'un acquittement est réalisé. L'acquittement de validation est réalisé en fonction du paramétrage à l'entrée ACK_NEC :

- si ACK_NEC = 0, l'acquittement est automatique
- si ACK_NEC = 1, vous devez acquitter à l'aide d'un front montant à l'entrée ACK pour valider.

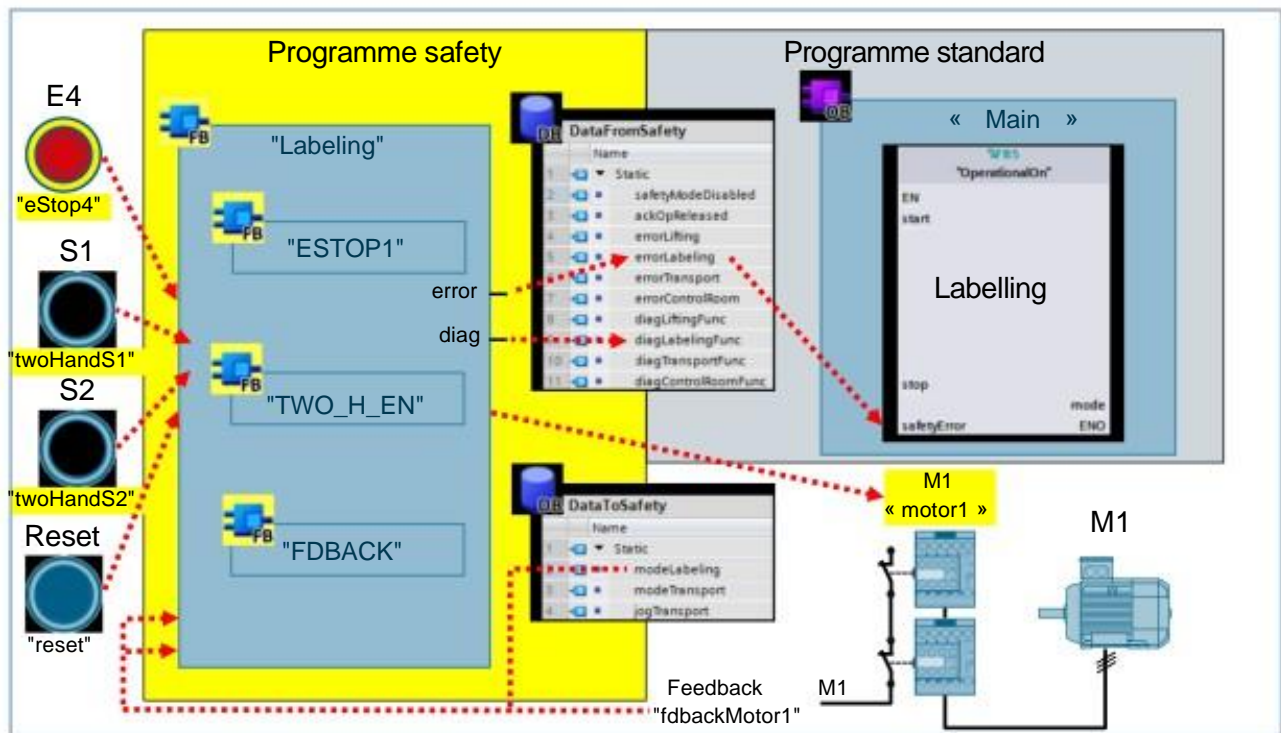
La sortie ACK_REQ signale qu'un acquittement utilisateur est nécessaire à l'entrée ACK. L'instruction met la sortie ACK_REQ à 1 dès que l'entrée E_STOP = 1.

Lorsque l'acquittement a été réalisé, l'instruction remet ACK_REQ à 0.

Attention :

Le paramétrage de la variable ACK_NEC = 0 n'est autorisé que lorsqu'un redémarrage automatique du processus correspondant est par ailleurs exclu.

6.31. Exercice 9 : Etiqueteuse



Enoncé

Dans la partie du site « Etiqueteuse » il faut étiqueter la pièce amenée. A l'instar de la partie de l'installation « Levage » nous ne traitons que la fonctionnalité de sécurité.

Le moteur de l'étiqueteuse ne doit rtre piloté que lorsque les conditions suivantes sont réalisées :

- Arrrt d'urgence (S-E4) est OK
- La commande bimanuelle est utilisée correctement ($t < 300\text{ms}$)
- Le mode automatique est actif

Le pilotage du moteur doit être surveillé par les contacts de retour des relais. Après l'appui de l'arrt d'urgence il ne faut libérer le pilotage du moteur qu'après acquittement. Le mode automatique de l'étiqueteuse doit rtre désactivé à la suite d'une coupure de sécurité.

Remarque : Lors de la programmation tenez compte des principaux aspects du guide de programmation comme la réutilisabilité et la structure du programme.

Procédure

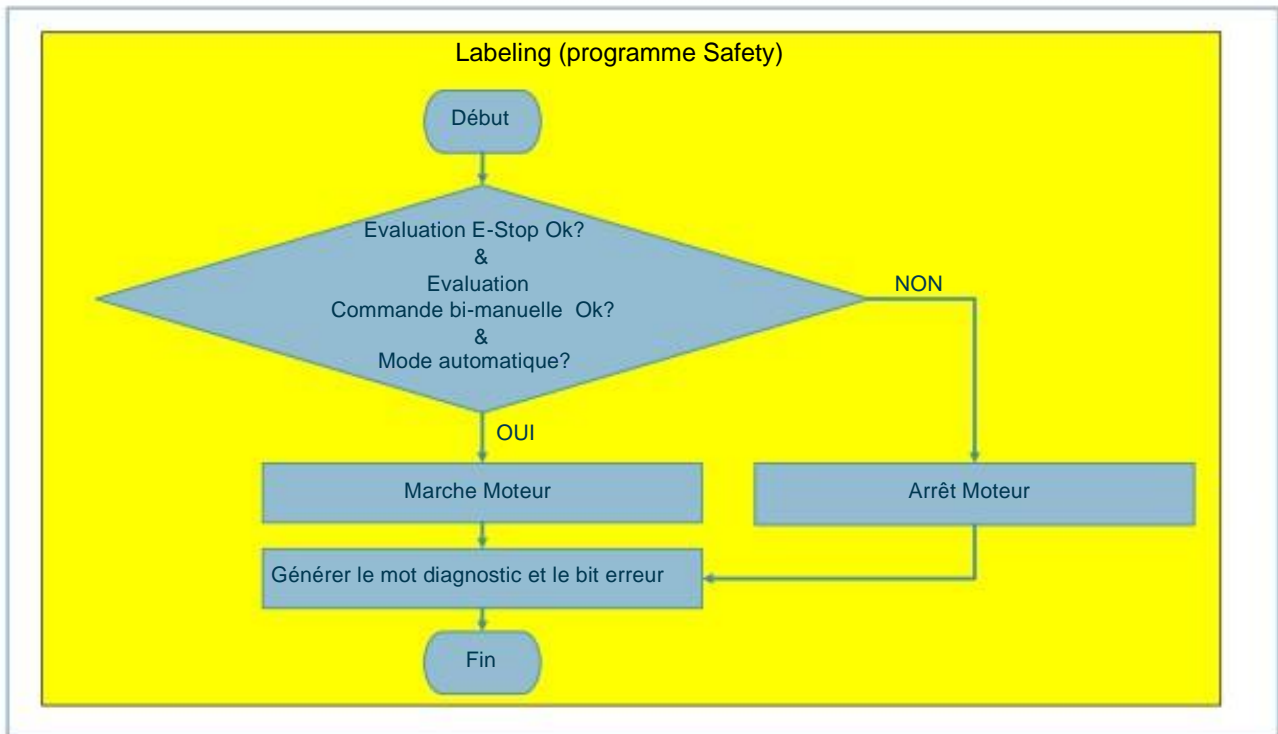
1. Bloc de fonction « Etiqueteuse » (description générale)

Créez un bloc de sécurité « Etiqueteuse » et programmez la fonctionnalité demandée (Enoncé). Pour l'évaluation utilisez les fonctions de sécurité « ESTOP1 », « TWO_H_EN ». Pour le pilotage du moteur vous utilisez la fonction de sécurité « FDBACK », car les retours des contacts peuvent être directement exploités (Temps de relecture = 200ms). L'acquittement de la fonction de sécurité est réalisé avec un bouton d'acquittement sur le banc de formation.

Implémentez également le diagnostic comme décrit dans l'exercice 8 (Chapitre 6.31.2) et transférez les données au bloc correspondant (Cf. vue).

Une description détaillée de l'exercice se trouve à la page suivante

6.31.1. Exercice 9: Organigramme



1. Bloc fonction « Etiqueteuse » (Description détaillée)

Créez un bloc de sécurité « Etiqueteuse » et appelez le bloc dans le programme de sécurité. Le bloc doit surveiller la libération du pilotage du moteur à l'aide des fonctions de sécurité «ESTOP », «TWO_H_EN » en mode de fonctionnement automatique. Groupez les conditions de validation et pilotez les contacteurs du moteur en utilisant la fonction de sécurité « FDBACK ».

« ESTOP » :

Dès que l'arrêt d'urgence E4 est actionné (« eStop4 » =0), la validation d'ESTOP doit être immédiatement bloquée (« ESTOP.Q » =0). Après le déverrouillage de l'arrêt d'urgence E4 (« eStop4 » =1), la validation d'ESTOP doit à nouveau être activée (« ESTOP.Q » =1) après actionnement du bouton d'acquiescement (« reset » =1).

« TWO_H_EN »

La validation (« TWO_H_EN.Q » = 1) ne doit intervenir que si le Bouton1 (« twoHandS1 ») et le Bouton2 (« twoHandS2 ») prennent la valeur 1 dans un intervalle de 300ms.

« FDBACK » :

Le moteur doit être pilotable avec les conditions nécessaires réunies :
 Arrêt d'urgence OK &
 Commande bimanuelle activée &
 Mode automatique Etiqueteuse ("DataToSafety".modeLabeling)

Le Moteur1 (« motor1 ») doit être commandé, via l'entrée « FDBACK.ON » =1 vous libérez la validation de la commande de la sortie « FDBACK.Q ».

Connectez correctement l'ensemble des interfaces concernées de « FDBACK » (fonction d'aide avec « F1 »). Le temps de surveillance « FDB_TIME » doit être réglé à 200ms.

Suite à la page suivante

Implémentez le diagnostic à la fin du bloc comme indiqué dans l'exercice 8 (Chapitre 6.31.2).

Enregistrez les données de diagnostic dans le bloc de données « DataFromSafety ».

"DataFromSafety".errorLabeling

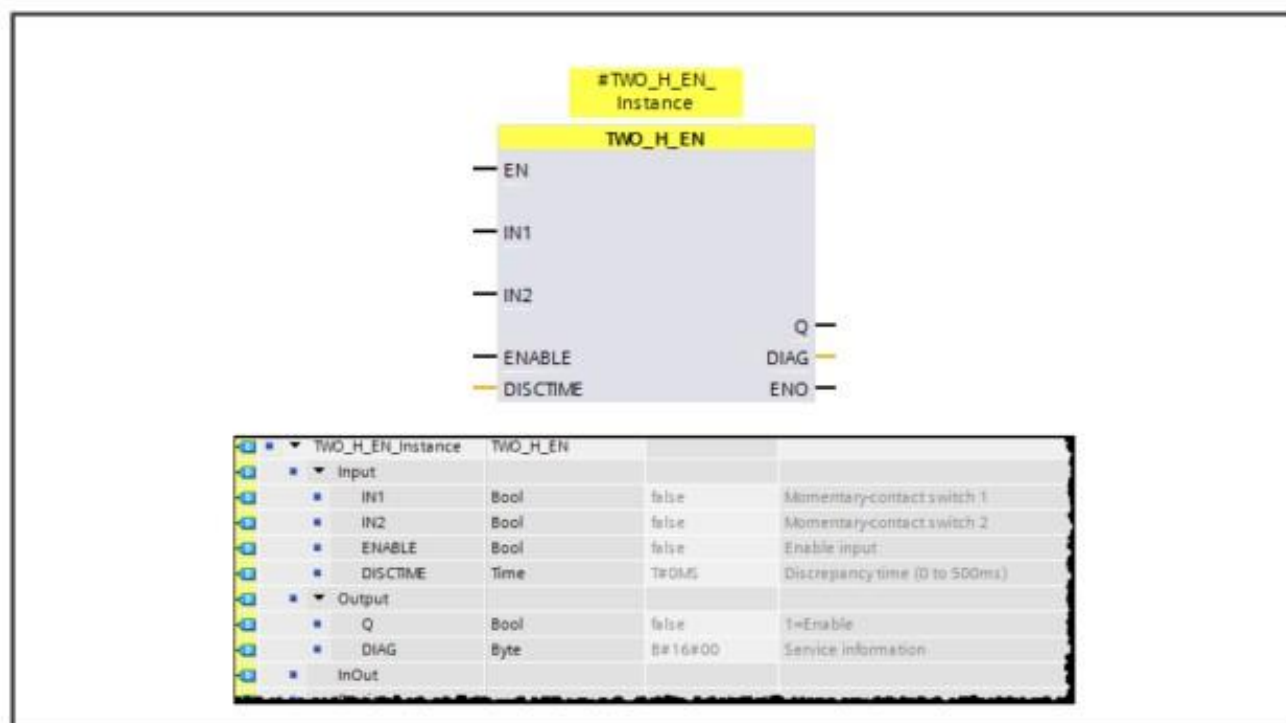
"DataFromSafety".diagLabelingFunc

Un arrêt en sécurité ("DataFromSafety".errorLabeling) doit également supprimer le mode automatique de l'étiqueteuse. Reliez le signal de mise à l'arrêt (errorLabeling) avec l'entrée « SafetyError » du bloc « OperationalOn » (Etiqueteuse).

2. Chargez l'ensemble des modifications dans la CPU
3. Enregistrez votre projet et testez le fonctionnement

Interfaces concernées		
Entrées	Standard	Sécurité
	« reset »	« "eStop4" »
	« fdbackMotor1 »	« "twoHandS1" »
		« "twoHandS2" »
		« "motor1VS" »
Sorties	Standard	Sécurité
		« "motor1" »
Blocs de données	Global	Système
	« "DataToSafety".modeLabeling »	
	« "DataFromSafety".errorLabeling »	
	« "DataFromSafety".diagLabelingFunc »	

6.31.2. La fonction de sécurité : TWO_H_EN



Cette instruction réalise une surveillance de commande bimanuelle avec validation.

Si les boutons IN1 et IN2 sont actionnés durant le temps de discordance autorisé DISCTIME ≤ 500 ms (IN1/IN2 = 1) (actionnement synchrone), le signal de validation Q passe à 1 si la validation est activée ENABLE = 1. Si la différence de temps entre l'actionnement du bouton IN1 et du bouton IN2 est supérieure à DISCTIME, les boutons doivent être relâchés et de nouveau actionnés.

Q est remis à 0 dès qu'un des boutons est relâché (IN1/IN 2 = 0) ou que la validation ne soit plus activée ENABLE = 0. Le signal de validation Q ne peut rtre à nouveau mis à 1 que si l'autre bouton a été relâché et que les deux boutons sont ensuite de nouveau actionnés avant l'écoulement du temps de discordance lorsque la validation ENABLE = 1.

6.31.3. La fonction de sécurité : FDBACK



Cette instruction réalise une surveillance de la boucle de retour.

A cet effet, le système vérifie l'égalité entre l'état de signal de la sortie Q et l'état de signal inversé de l'entrée de lecture de retour FEEDBACK. La sortie Q est mise à 1 dès que l'entrée ON = 1. La condition est que l'entrée de lecture de retour FEEDBACK = 1 et qu'aucune erreur de lecture de retour ne soit enregistrée. La sortie Q est remise à 0 dès que l'entrée ON = 0 ou lorsqu'une erreur de lecture de retour est détectée.

Une erreur de lecture de retour ERROR = 1 est détectée lorsque l'état de signal inversé de l'entrée de lecture de retour FEEDBACK (de la sortie Q) ne suit pas l'état de signal de la sortie Q avant l'écoulement du temps de lecture de retour FDB_TIME maximal toléré. L'erreur de lecture de retour est enregistrée.

Si une discordance entre l'entrée de lecture de retour FEEDBACK et la sortie Q est détectée après une erreur de lecture de retour, l'erreur de lecture de retour est acquittée en fonction du paramétrage de ACK_NEC :

- si ACK_NEC = 0, l'acquiescement est automatique
- si ACK_NEC = 1, vous devez acquiescer l'erreur de lecture de retour à l'aide d'un front montant à l'entrée ACK.

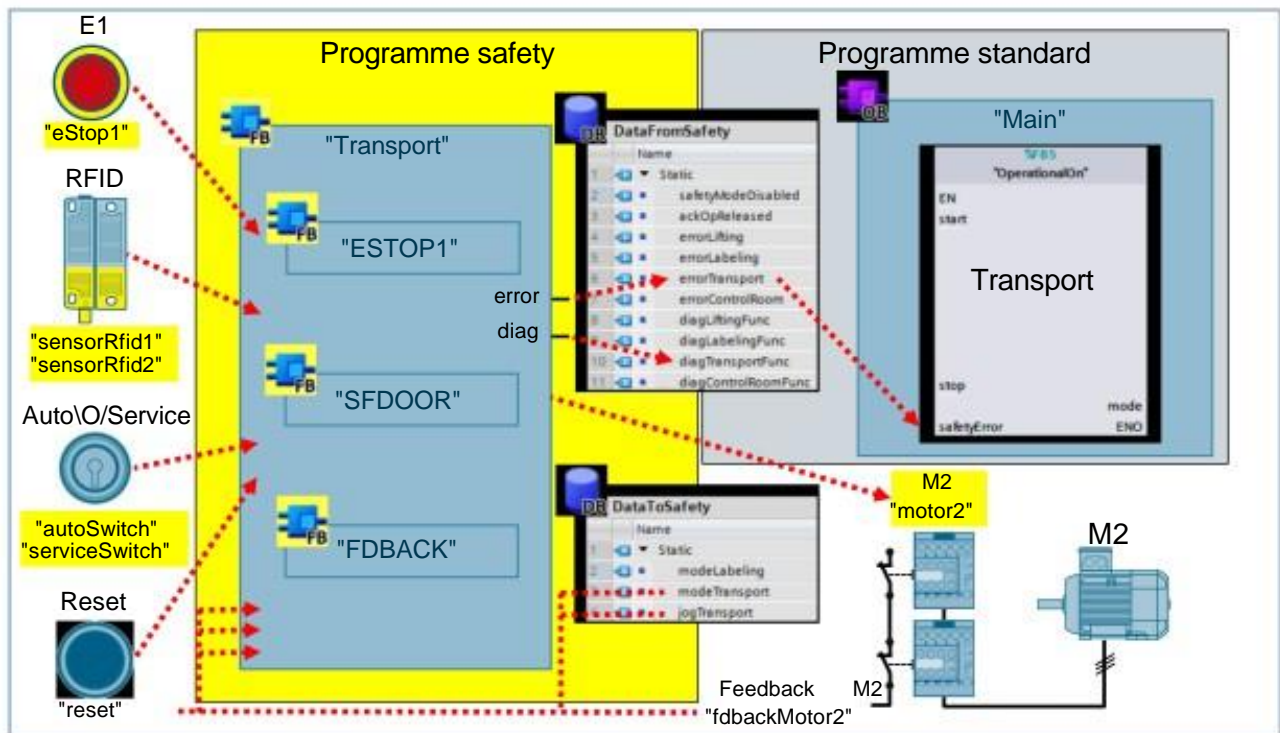
La sortie ACK_REQ = 1 signale qu'un acquiescement utilisateur est nécessaire à l'entrée ACK pour acquiescer l'erreur de lecture de retour. Une fois l'acquiescement réalisé, l'instruction remet ACK_REQ à 0.

Pour qu'aucune erreur de lecture de retour ne soit détectée lors d'une passivation de la périphérie de sécurité commandée par la sortie Q et qu'aucun acquiescement ne soit requis, vous devez connecter l'entrée QBAD_FIO au signal QBAD de la périphérie de sécurité correspondante ou au signal QBAD_Q_xx, à l'état de la valeur inversé du canal correspondant.

Attention !

Le paramétrage de la variable ACK_NEC = 0 n'est autorisé que si un redémarrage automatique du processus correspondant est exclu par ailleurs.

6.32. Exercice 10: Transport



Enoncé

Dans la partie Transport il faut évacuer la pièce réalisée. Ici ne seront considérées que les fonctionnalités relevant de la sécurité.

Le moteur du transport ne doit être commandé que si les conditions suivantes sont satisfaites :

- Arrêt d'urgence (E1) en fonction
- La porte de protection est fermée
- Le commutateur de sécurité est positionné en mode auto (Auto)
- Le mode de fonctionnement automatique est activé.

Il faut en outre, assurer la possibilité de commander le transport par à coup dans les phases de maintenance et de mise en service avec la porte de protection ouverte avec les conditions satisfaites suivantes :

- Arrêt d'urgence (E1) en fonction
- Le commutateur de sécurité est positionné sur Maintenance (Service)
- Le mode automatique n'est pas activé (Arrêt)
- Le bouton « Pas à pas » est piloté sur l'IHM

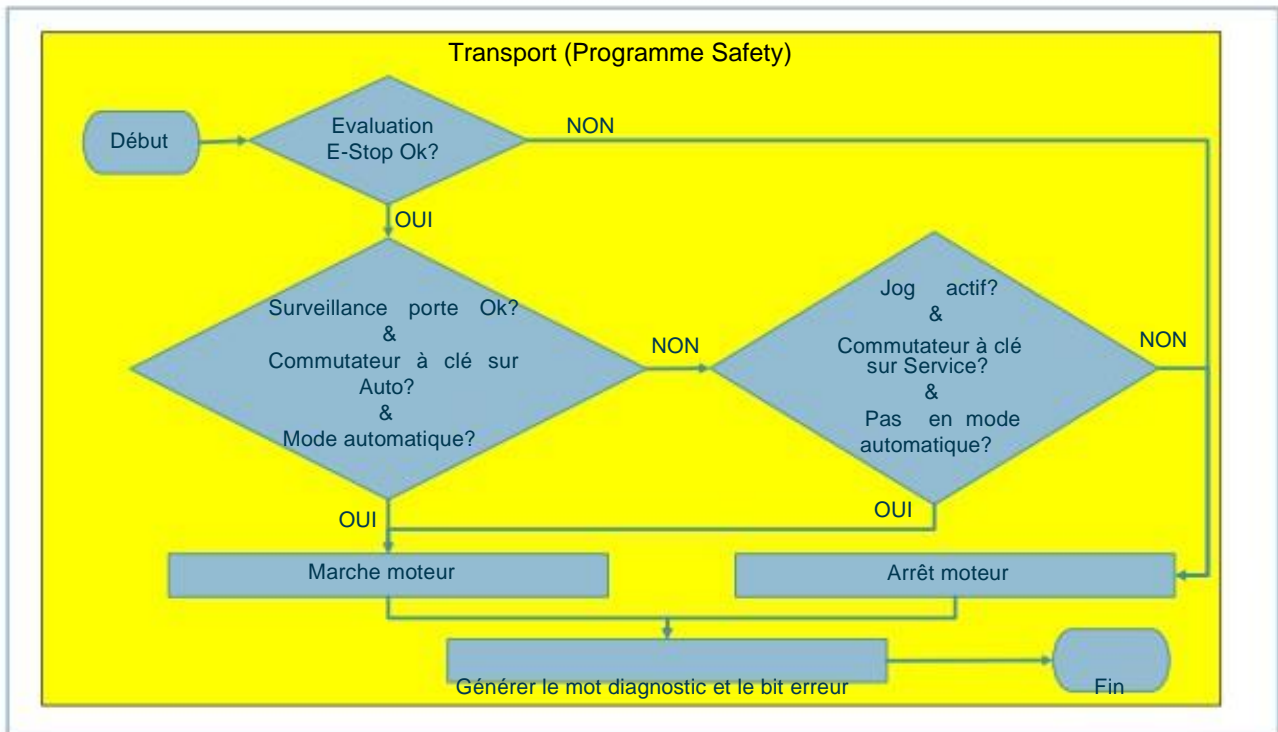


La commande du moteur doit être surveillée par les contacts de relecture des contacteurs. Après un déclenchement de l'arrêt d'urgence ou l'ouverture de la porte de sécurité, la validation du pilotage du moteur doit uniquement intervenir après acquittement. Le mode automatique du transport doit être désactivé lors d'une coupure de sécurité.

Remarque : Lors de la programmation tenez compte des principaux aspects du guide de programmation comme la réutilisabilité et la structure du programme.

Suite à la page suivante

6.32.1. Exercice 10 : Organigramme



Procédure

1. Bloc de fonction « "Transport" » (Description générale)

Insérez le bloc fonction de sécurité « "Transport" » et programmez la fonctionnalité demandée (Enoncé). Utilisez pour évaluation les fonctions de sécurité « "ESTOP1" », « "SFDOOR" ».

Pour la commande du moteur, utilisez la fonction de sécurité « "FDBACK" », car on peut y évaluer directement les contacts de relecture (Temps de relecture=200ms).

L'acquiescement de la fonction de sécurité est réalisé par le bouton d'acquiescement du banc de formation.

Implémentez également le diagnostic comme décrit dans l'exercice 8 (Chapitre 6.31.2) et transférez les données au bloc de donnée concerné (Cf. vue).

1. Bloc de fonction « "Transport" » (description détaillée)

Insérez le bloc de sécurité « "Transport" » et appelez le bloc dans le programme de sécurité. Le bloc doit surveiller la validation du pilotage du moteur avec les fonctions de sécurité « "ESTOP" », « "SFDOOR" », un commutateur à clé et le mode de fonctionnement activé. regroupez l'ensemble des conditions de validation et commandez le moteur (contacteurs) à l'aide de la fonction de sécurité « "FDBACK" ».

« ESTOP » :

Dès que l'arrêt d'urgence E1 est actionné (« "eStop1" » = 0) la validation d'ESTOP doit être immédiatement bloquée (« ESTOP.Q » = 0). Après le déverrouillage de l'arrêt d'urgence E1 (« "eStop1" » = 1) la validation d'ESTOP doit à nouveau être débloquée (« "ESTOP.Q" » = 1) après appui du bouton d'acquiescement (« "reset" » = 1).

« SFDOOR » :

La validation (« SFDOOR.Q » = 1) ne doit intervenir que lorsque la porte de protection est complètement fermée (« sensorRfid1 » = 1 et « sensorRfid2 » = 1). La fonctionnalité « ouverture nécessaire pour démarrage » n'est pas nécessaire (« SFDOOR.OPEN_NEC » = 0). Après la fermeture de la porte de protection, la validation ne doit intervenir qu'après l'actionnement du bouton d'acquiescement (« reset » = 1).

Suite page suivante

« FDBACK » :

Le moteur2 doit être commandé dès que les conditions nécessaires pour le mode automatique sont remplies :

Arrrt d'urgence OK &
 Porte de protection fermée &
 Mode automatique « Transport » ("DataToSafety".modeTransport = 1) &
 Commutateur à clé en mode Auto ("autoSwitch")

OU mode maintenance

Arrrt d'urgence OK &
 Arrêt Transport ("DataToSafety".modeTransport =0) &
 Commutateur à clé en position Maintenance ("serviceSwitch") &
 « marche par à-coups » actif via l'IHM ("DataToSafety".jogTransport)

Via l'entrée « FDBACK.ON » =1 libérez la commande de la sortie « FDBACK.Q ».
 Connectez correctement toutes les interfaces des « FDBACK » (fonction d'aide par F1). Le temps de surveillance « FDB_TIME » doit être réglé à 200ms.

Implémentez le diagnostic à la fin du bloc comme indiqué dans l'exercice 8 (Chapitre 6.31.2).
 Enregistrez les données de diagnostic dans le bloc de données « DataFromSafety ».

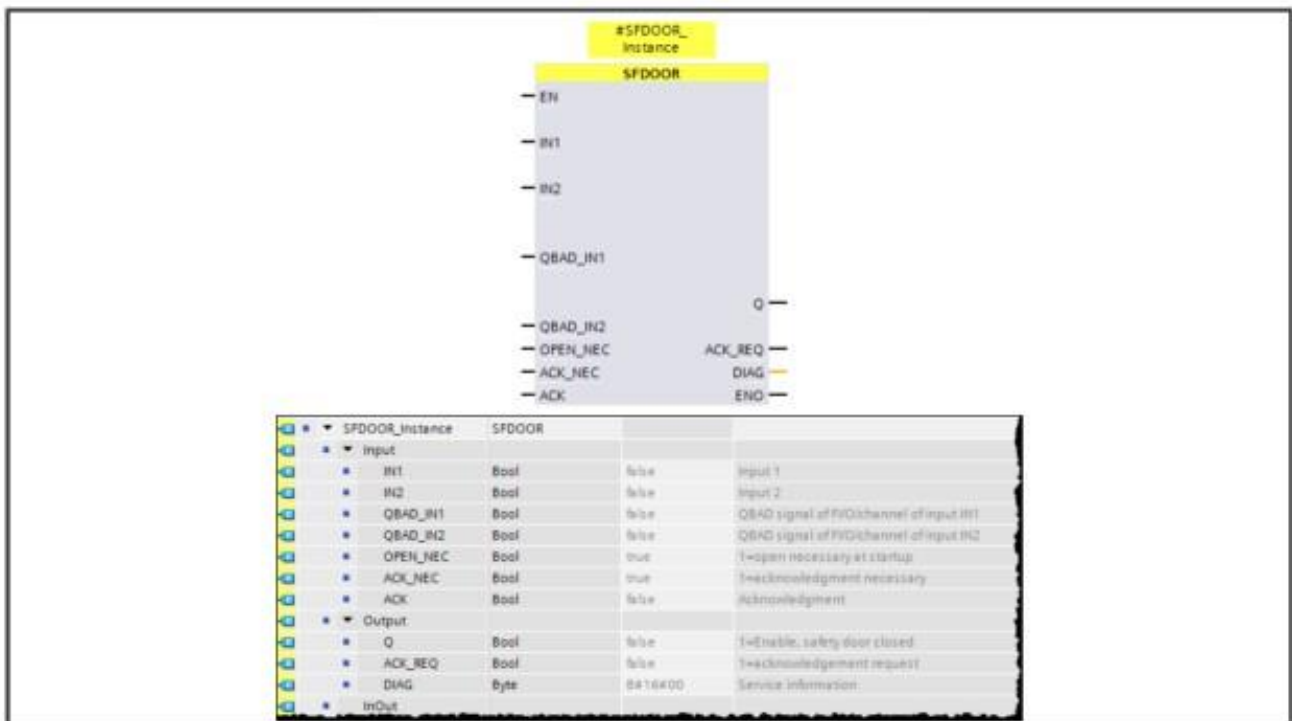
"DataFromSafety".errorTransport
 "DataFromSafety".diagTransportFunc

Un arrêt en sécurité ("DataFromSafety".errorTransport) doit également supprimer le mode automatique du transport. Reliez le signal de mise à l'arrt (errorTransport) avec l'entrée « SafetyError » du bloc « OperationalOn » (Transport).

2. Chargez l'ensemble des modifications dans la CPU.
3. Enregistrez votre projet et testez le fonctionnement.

Interfaces concernées		
Entrées	Standard	Sécurité
	"reset"	"eStop1"
	"fdbackMotor2"	"sensorRfid1"
		"sensorRfid2"
		"autoSwitch"
		"serviceSwitch"
		"sensorRfid1VS"
		"sensorRfid2VS"
		"motor2VS"
Sorties	Standard	Sécurité
		"motor2"
Blocs de données	Global	Système
	"DataToSafety".modeTransport	
	"DataToSafety".jogTransport	
	"DataFromSafety".errorTransport	
	"DataFromSafety".diagTransportFunc	

6.32.2. La fonction de sécurité : SFDOOR



Cette instruction réalise une surveillance de la porte de protection.

Le signal de validation Q est remis à 0 dès qu'une des deux entrées IN1 ou IN2 prend l'état de signal 0 (la porte de protection est ouverte). Le signal de validation ne peut être remis à 1 que lorsque :

- les deux entrées IN1 et IN2 ont pris l'état de signal 0 avant la fermeture de la porte (la porte de protection a été entièrement ouverte)
- les deux entrées IN1 et IN2 prennent ensuite l'état de signal 1 (la porte de protection est fermée)
- un acquittement est réalisé

L'acquittement de validation est réalisé en fonction du paramétrage à l'entrée ACK_NEC :

- si ACK_NEC = 0, l'acquittement est automatique
- si ACK_NEC = 1, vous devez acquitter la validation à l'aide d'un front montant à l'entrée ACK.

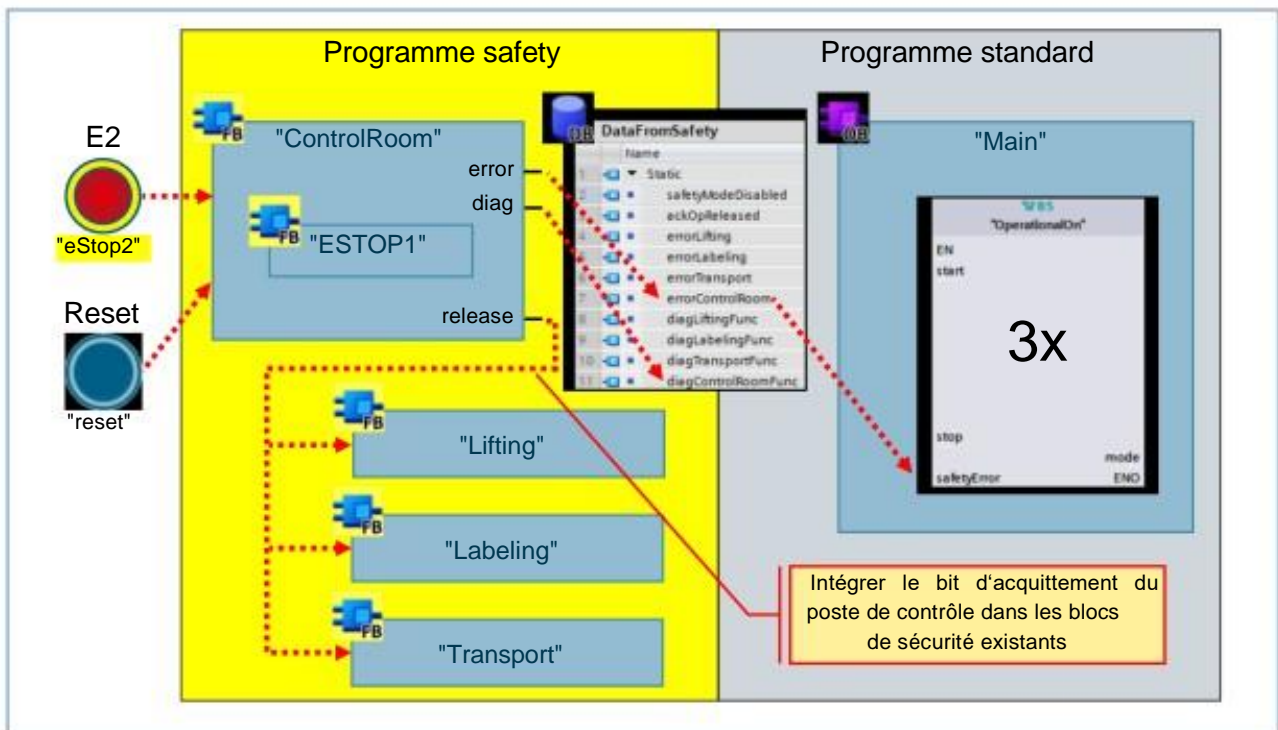
La sortie ACK_REQ = 1 signale que l'acquittement nécessite un acquittement utilisateur à l'entrée ACK. L'instruction met ACK_REQ à 1 dès que la porte est fermée. Lorsque l'acquittement a été réalisé, l'instruction remet ACK_REQ à 0.

Pour que l'instruction détecte si les entrées IN1 et IN2 sont à 0 uniquement en raison d'une passivation de la périphérie de sécurité correspondante, vous devez connecter les entrées QBAD_IN1 ou QBAD_IN2 au signal QBAD de la périphérie de sécurité correspondante ou au signal QBAD_I_xx à l'état de la valeur inversé des canaux correspondants. Ceci vous permet entre autres d'éviter de devoir ouvrir entièrement la porte de protection avant un acquittement en cas de passivation de la périphérie de sécurité.

Attention !

Le paramétrage de la variable ACK_NEC = 0 n'est autorisé que lorsqu'un redémarrage automatique du processus correspondant est totalement exclu par ailleurs.

6.33. Exercice 11 : Poste de contrôle



Enoncé

Le poste de contrôle sert à surveiller l'ensemble de l'installation. Le poste de contrôle doit avoir la possibilité d'amener l'installation dans un état sûr à l'aide de l'arrêt d'urgence. Lorsque l'arrêt d'urgence est actionné, toutes les parties de l'installation (Dispositif de levage, Etiqueteuse et Transport) doivent passer en situation de sécurité.

Après le déclenchement de l'arrêt d'urgence, la validation ne peut intervenir qu'après un acquiescement.

L'ensemble des parties en mode automatique doivent pouvoir être réinitialisé par le poste de contrôle à la suite d'un arrêt de sécurité.

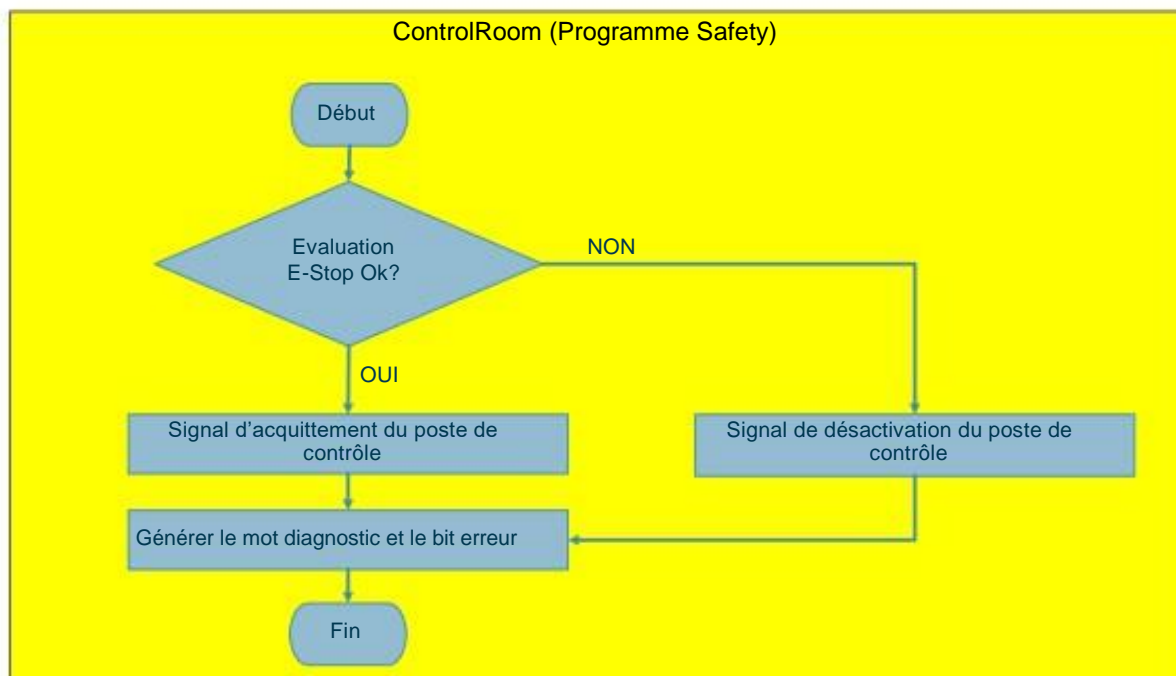
Procédure

1. Bloc fonction « Poste de contrôle » (description générale)

Créez le bloc de fonction de sécurité « Poste de contrôle » et programmez la fonctionnalité requise (Enoncé). Utilisez pour évaluation de l'arrêt d'urgence la fonction de sécurité « ESTOP1 » de la liste d'instructions. L'acquiescement de la fonction de sécurité est réalisé par le bouton d'acquiescement du banc de formation. Implémenter également le diagnostic comme décrit dans l'exercice 8 (Chapitre 6.31.2) et transférez les données dans le bloc de données correspondant (Cf. vue).

La description détaillée de l'exercice se trouve à la page suivante

6.33.1. Exercice 11 : Organigramme



1. Bloc de fonction « Poste de contrôle » (description détaillée)

Le bloc doit surveiller l'arrêt d'urgence E2 (« "eStop2" ») à l'aide de la fonction de sécurité (ESTOP1). Dès que l'arrêt d'urgence E2 est actionné (« "eStop2" » = 0) il faut immédiatement engager l'arrêt de sécurité.

Transférez le signal de coupure (ESTOP1.Q) à toutes les parties de l'installation. Utilisez pour cela les interfaces (Entrées et sorties) du bloc de fonction (cf. vue).

Complétez les blocs « Dispositif de levage », « Etiqueteuse » et « Transport » avec cette nouvelle condition d'acquiescement.

Implémentez le diagnostic à la fin du bloc comme décrit dans l'exercice 8 (Chapitre 6.31.2).

Enregistrer les données de diagnostic dans le bloc de données « DataFromSafety ».

"DataFromSafety".errorControlRoom

"DataFromSafety".diagControlRoomFunc

Un arrêt de sécurité ("DataFromSafety".errorControlRoom) doit également assurer la suppression de l'ensemble des modes automatiques. Affectez le signal de coupure (errorControlRoom) aux entrées « SafetyError » des blocs « OperationalOn ».

2. Chargez toutes les modifications dans la CPU
3. Sauvegardez le projet et testez la fonctionnalité

Interfaces concernées		
Entrées	Standard	Sécurité
	"reset"	"eStop2"
Sorties	Standard	Sécurité
Blocs de données	Global	Système

6.34. Aperçu des exercices complémentaires

Les exercices complémentaires sont indépendants l'un par rapport à l'autre et peuvent être réalisés suivant pertinence ou intérêt.

Exercice complémentaire 1

- Visualisation des informations du groupe d'exécution

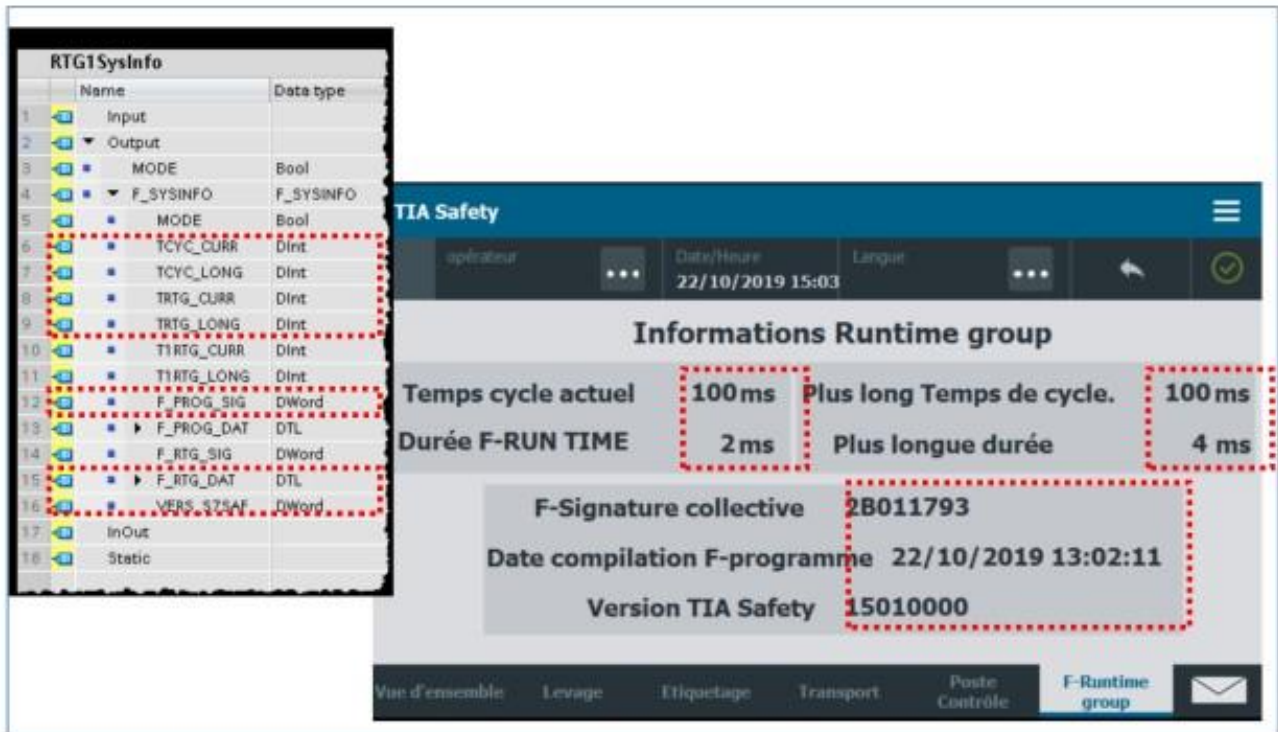
Exercice complémentaire 2

- Acquiescement global de la périphérie de sécurité

Exercice complémentaire 3

- Acquiescement de sécurité via l'IHM

6.34.1. Exercice complémentaire 1 : Visualisation des informations du groupe d'exécution



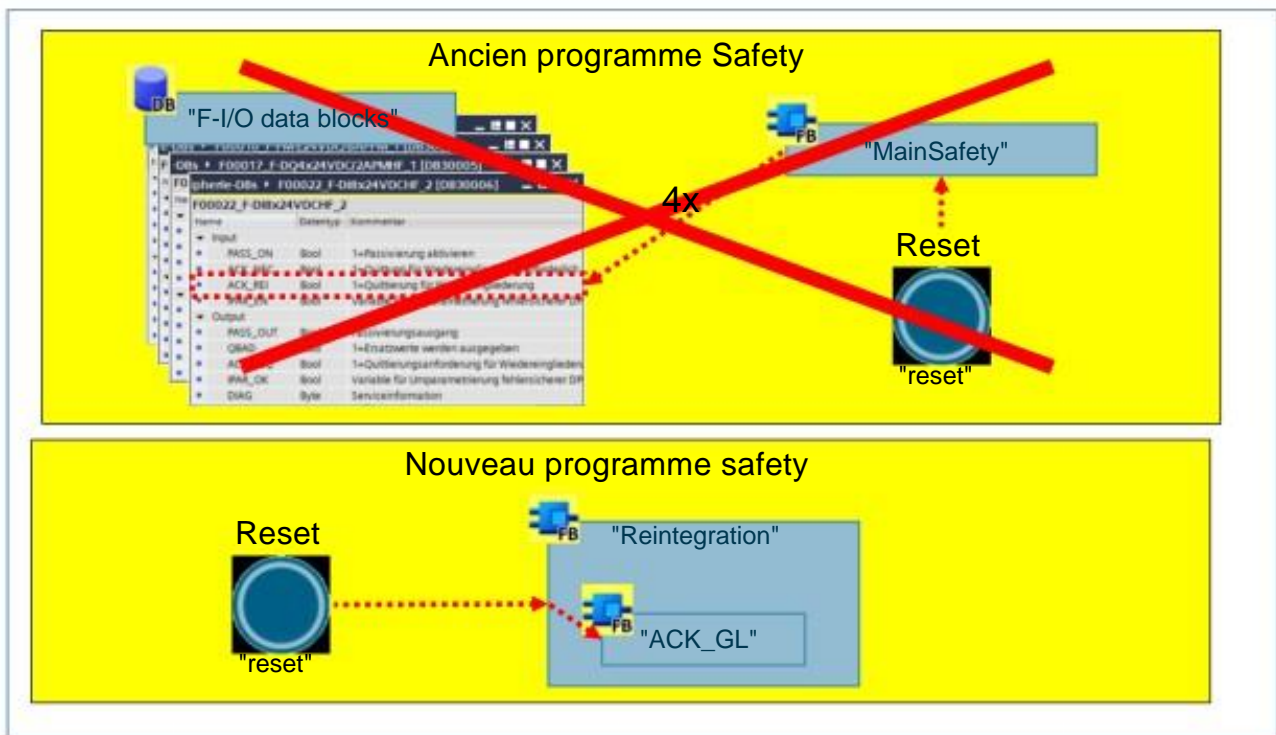
Enoncé

Toutes les informations pertinentes au sujet du programme de sécurité doivent être accessibles au niveau de l'IHM.

Procédure

1. Dans le projet IHM actuel se trouve la vue « 15_Info » (Cf. Image). Cette vue est appelée par le bouton « Groupe d'exécution F » dans le Panel. Insérez les champs de sortie individuels, relatifs aux liaisons correctes avec les variables du bloc de données système « RTG1SysInfo » de la CPU.
Remarque : Tenez compte du typage des données pour les variables du bloc de données système. Eventuellement il faudra corriger les champs de sortie de l'IHM en fonction des formats de visualisation et de présentation.
2. Transférez votre projet IHM dans le Panel.
3. Enregistrez votre projet et testez la fonctionnalité

6.34.2. Exercice complémentaire 2 : Acquittement global de la périphérie de sécurité



Enoncé

Actuellement, l'acquiescement de toutes les périphéries F du programme de sécurité est réalisé dans « MainSafety » par une commande directe dans chaque DB F de périphérie. Cet acquiescement doit être remplacé par la fonction de sécurité « ACK_GL ».

Avantages :

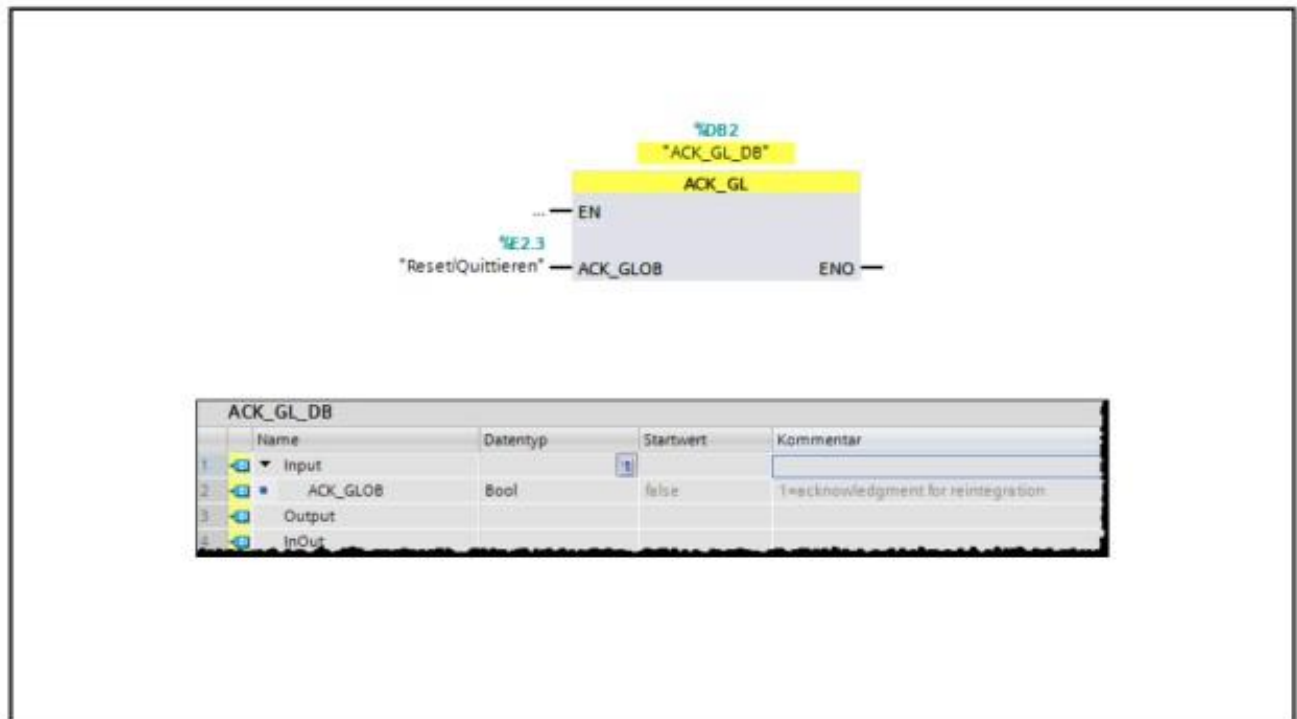
- Acquiescement global de la périphérie F avec une fonction de sécurité certifiée
- L'acquiescement d'une périphérie F ajoutée ultérieurement sera automatiquement intégré.

Remarque : Le bloc n'acquiesce que la périphérie F. L'acquiescement de fonctions de sécurité comme ESTOP1, SFDOOR ou FDBACK doit être programmé par l'utilisateur.

Procédure

1. Effacez la programmation actuelle des acquiescements.
2. Insérez le bloc « Reintegration » et appelez-le au niveau du programme de sécurité.
Remarque : Le bloc « Reintegration » est déjà préprogrammé pour l'exercice complémentaire 3. La fonction de sécurité « ACK_GL » peut aussi être appelée directement dans le programme de sécurité.
3. Programmez l'acquiescement global avec la fonction de sécurité « ACK_GL » dans le bloc « Reintegration ». L'acquiescement est toujours réalisé avec le bouton d'acquiescement « reset ». (Cf Vue)
4. Transférez les modifications dans la CPU.
5. Enregistrez votre projet et testez la fonctionnalité

6.34.2.1. La fonction de sécurité : ACK_GL



Cette instruction génère un acquittement pour la réintégration simultanée de toutes les périphéries / de tous les canaux de la périphérie de sécurité d'un groupe d'exécution F après des défauts de communication ou des défauts de périphérie de sécurité ou de canaux.

Un acquittement utilisateur via un front montant à l'entrée ACK_GLOB est nécessaire pour la réintégration. L'acquittement s'effectue de la même manière que l'acquittement utilisateur via la variable ACK_REI du DB de périphérie de sécurité, mais agit simultanément sur toutes les périphéries de sécurité du groupe d'exécution F dans lequel l'instruction est appelée.

Lorsque vous utilisez l'instruction ACK_GL, il n'est pas nécessaire de prévoir un acquittement utilisateur via la variable ACK_REI du DB de périphérie de sécurité pour chaque périphérie de sécurité du groupe d'exécution F (F-runtime group).

6.34.3. Exercice supplémentaire 3 : acquittement de sécurité avec l'IHM



Enoncé

Actuellement, l'acquittement de la périphérie F ou de la fonction de sécurité est uniquement réalisée par le bouton d'acquittement « Reset » du banc de test. Comme le pilotage de l'installation a lieu essentiellement par l'IHM, il s'agit de programmer un acquittement avec l'IHM. Utilisez pour cela la fonction de sécurité « ACK_OP » afin de s'assurer que l'acquittement ne soit réalisé par inadvertance ou via un signal binaire simple.

Représentation dans l'IHM

Le poste de commande permet à l'utilisateur de réaliser avec deux boutons soit l'acquittement de la périphérie F (« Acquittement Périphérie F ») ou l'acquittement des fonctions de sécurité (« Acquittement des fonctions Safety »). Les boutons sont uniquement opérationnels quand une demande d'acquittement est présente. → la suite de l'actionnement s'ouvre un Pop-Up qui réalise l'acquittement en deux étapes :

- Etape 1 : L'IHM transmet la valeur 6 (Integer) au programme de sécurité « ACK_OP »
- Etape 2 : L'IHM transmet, avant l'écoulement de 60s, une deuxième valeur (Integer) au programme de sécurité « ACK_OP ». (Périphérie F = 9, Fonctions de sécurité = 23)

Remarque : La présentation de l'IHM est presque entièrement réalisée. Il reste les boutons pour acquittement et quelques liaisons aux variables IHM à mettre en place (voir réalisation).

Extension du programme de sécurité

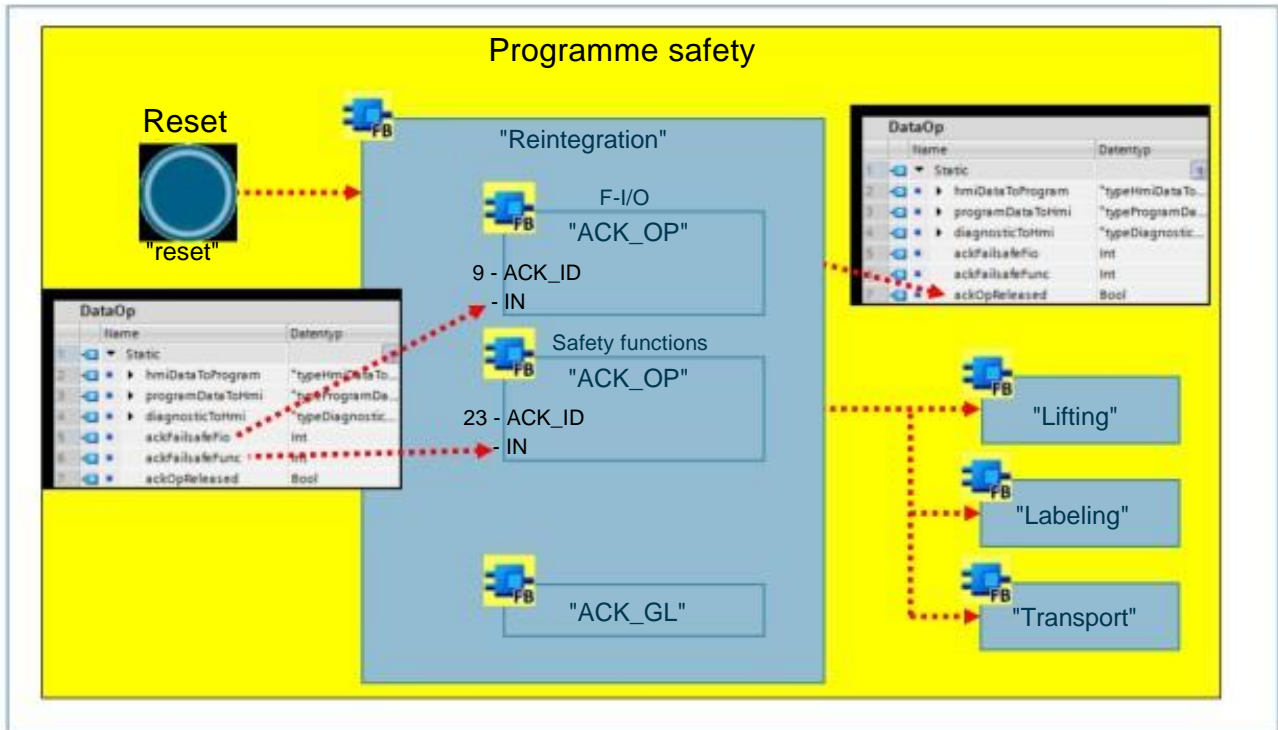
Le programme de sécurité avec la fonction « ACK_OP » doit exécuter les étapes de l'acquittement par l'IHM et ainsi fournir une validation de l'acquittement. Cela nécessite deux appels de « ACK_OP » car la périphérie F et les fonctions de sécurité nécessitent un acquittement séparé. Les validations des blocs « ACK_OP » réaliseront les acquittements respectifs.

Réalisation

1. Copier les boutons pour acquittement de la bibliothèque « Exercices Optionnels-> Exercice_3 » aux emplacements respectifs dans la vue IHM « 14_Salle de Contrôle » (Cf. Vue)

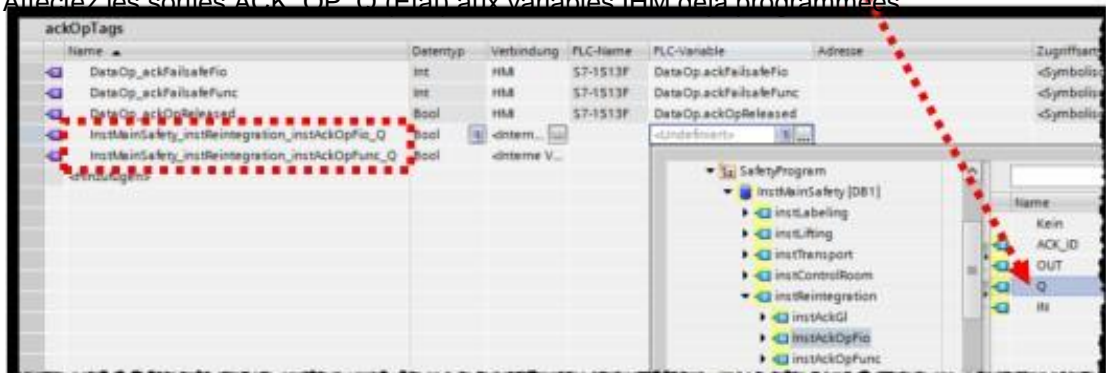
Suite page suivante

6.34.3.1. Exercice complémentaire 3 : Extension du programme



Réalisation

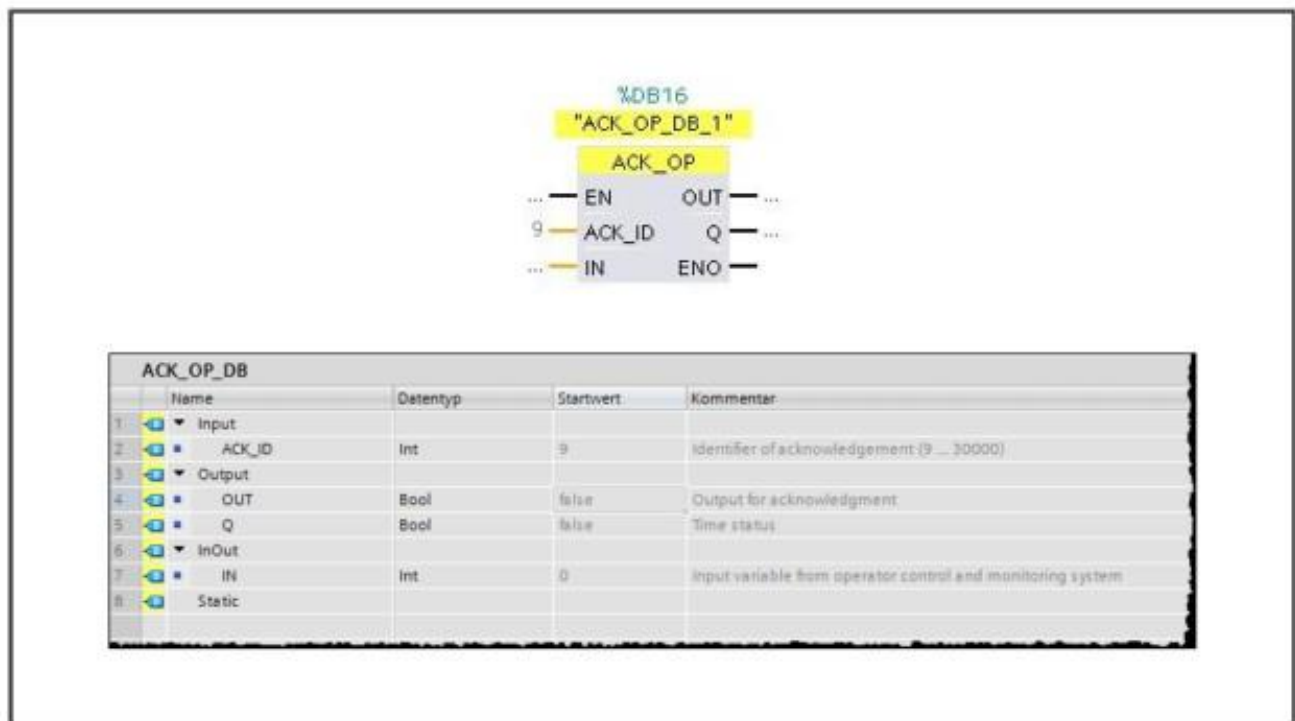
1. Intégrez deux appels de la fonction de sécurité « ACK_OP » dans le bloc « Reintegration ».
2. Affectez les entrées des blocs comme indiqué dans la vue.
3. Les sorties de validation ACK_OP.OUT servent maintenant d'acquiescement supplémentaire par rapport au bouton « Reset » déjà mis en place. Adaptez votre programme dans ce sens. Remarque : Tenez compte du fait que les deux sorties de validation ne présentent pas les mêmes fonctionnalités. Il s'agit soit de l'acquiescement de la périphérie F soit de celui des fonctions de sécurité.
4. Transférez les sorties de validation « ACK_OP.OUT » à l'IHM via la variable « "DataOP".ackOpReleased ». Dès la présence d'une des sorties (ACK_OP.OUT) il faut activer « "DataOP".ackOpReleased ». Remarque: le transfert est nécessaire pour les vues Pop-Up dans l'IHM.
5. Affectez les sorties ACK_OP.Q (Etat) aux variables IHM déjà programmées



Remarque : le transfert est nécessaire aux vues Pop-Up de l'IHM

6. Chargez les modifications dans la CPU et testez la fonctionnalité.

6.34.3.2. La fonction de sécurité : ACK_OP



Cette instruction permet d'effectuer un acquittement de sécurité à partir d'un système de contrôle-commande.

Il est possible par ex. de commander la réintégration de la périphérie de sécurité à partir du système de contrôle-commande. Un acquittement comprend deux étapes :

- Passage de la variable « IN » à la valeur 6 pendant exactement un cycle
- Passage de la variable « IN » à la valeur présente à l'entrée ACK_ID avant l'écoulement d'un intervalle d'une minute

L'instruction détermine si, une fois que l'entrée/sortie IN a pris la valeur 6, elle reprend la valeur présente à l'entrée ACK_ID après 1 seconde au plus tôt et 1 minute au plus tard. La sortie OUT (sortie d'acquiescement) est ensuite mise à 1 durant un cycle.

Si vous entrez une valeur invalide ou si l'entrée/sortie IN ne prend pas la valeur présente à l'entrée ACK_ID durant un intervalle d'une minute ou avant écoulement d'une seconde, alors le paramètre in/out « IN » sera réinitialisée à 0 et les deux étapes précédentes devront être renouvelées. La sortie Q est mise à 1 pendant l'intervalle dans lequel doit s'effectuer le passage de 6 à la valeur présente à l'entrée ACK_ID. Sinon, Q a la valeur 0.

6.35. Informations complémentaires



6.35.1. Liens

Généralités

[Siemens Industry Online Support \(SIOS\)](#)

[Programming Guidelines and Programming Styleguide \(ID:81318674\)](#)

[An Overview of the Most Important Documents and Links - Safety \(ID: 90939626\)](#)

FAQ

[Which modules can be operated in the load group of the power module F-PM-E PPM of the ET 200SP? \(ID:83203124\)](#)

[How do you assign PROFIsafe addresses so that they are unique network-wide and CPU-wide? \(ID:109740240\)](#)

[What should you watch out for when selecting the operating mode in conjunction with functional safety? \(ID:89260861\)](#) [How do you incorporate fail-safe, inductive, clocked switches in STEP 7 Safety? \(ID:109736836\)](#)

Exemples d'application

[Configuration Control with SIMATIC S7 \(ID:29430270\)](#)

[SIMATIC S7-1500 Profiling \(ID:29430270\)](#)

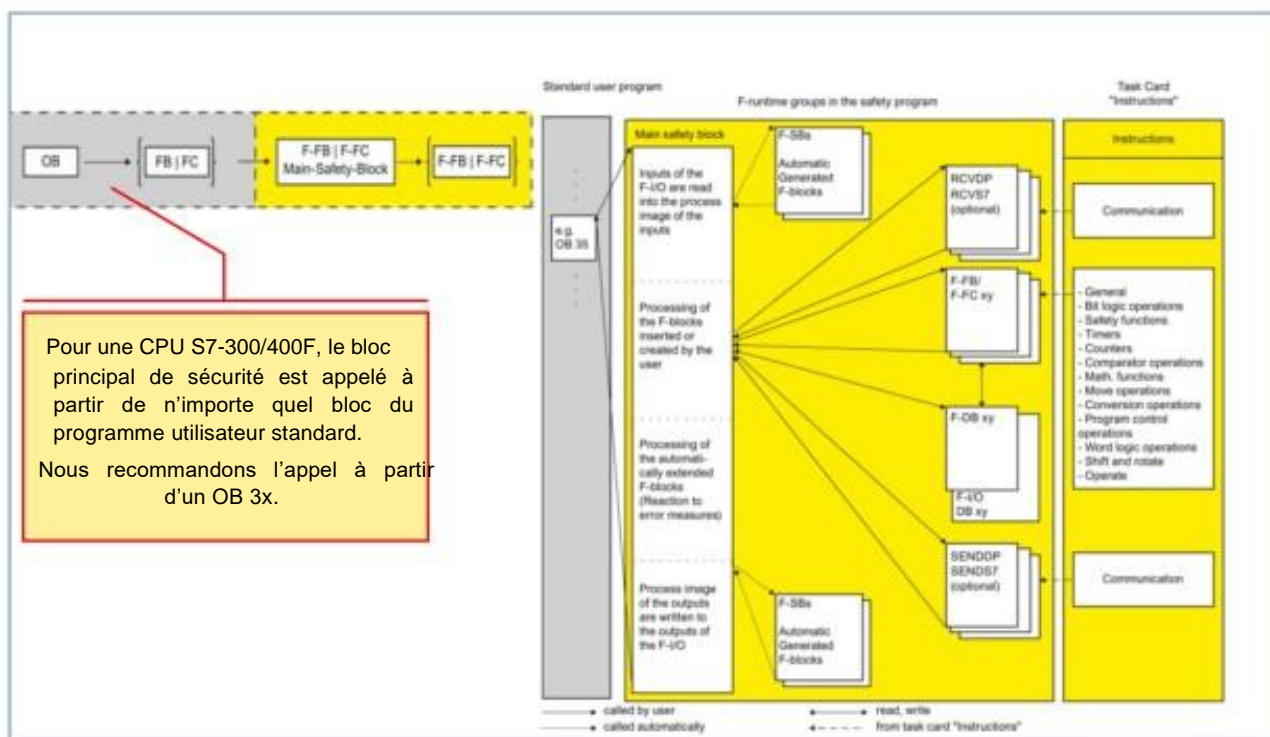
[Failsafe library LDrvSafe to control the Safety Integrated functions of the SINAMICS drive family \(ID:109485794\)](#)

[SINAMICS S: S110/S120 Safety Acceptance Test \(ID:52248627\)](#)

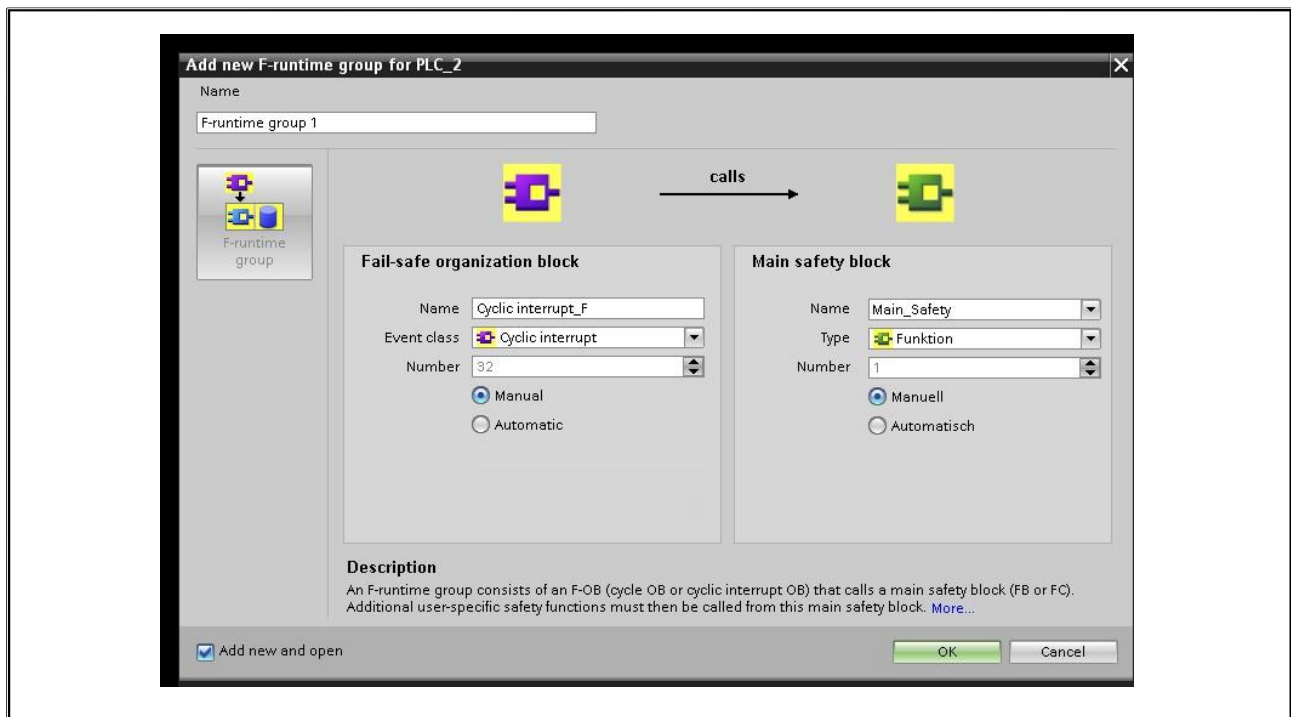
[Safety position, standstill, direction and speed detection \(ID:49221879\)](#)

[Library of general functions \(LGF\) for SIMATIC STEP 7 \(TIA Portal\) and SIMATIC S7-1200 / S7-1500 \(ID: 109479728\)](#) [Guide to Standardization \(ID: 109756737\)](#)

6.35.2. Structure et traitement du programme de sécurité (300F/400F)



6.35.3. Groupe séquentiel (300F/400F)



6.35.4. F_GLOBDB (300F/400F)

The screenshot shows the SIMATIC Manager interface. On the left, the project tree displays the hierarchy: PLC_1 [CPU 317F-2 DP/DP] > Blocs de programme > Main [OB1]. The main window shows the 'F_GLOBDB' data block definition. It is a static block with the following fields:

Num	Nom	Type de données	Décalage	Valeur de départ	Rétention	Visible da...	Valeur de ...	Cor
1	Static							
2	F_PROG_SIG	DWord	2.0	DWR16x64x2...				
3	MODE	Bool	36.0	false				
4	TESTM	Bool	36.1	false				
5	ERROR	Bool	36.2	false				
6	VKE0	Bool	36.3	false				
7	VKE1	Bool	36.4	true				
8	F_PROG_SIG	Date_And_Time	38.0	DT#17-5-23-12...				

A red dashed box highlights the VKE0 and VKE1 fields. An arrow points from this box to a ladder logic network labeled 'Réseau 1 :'. The network contains two normally open contacts in series. The first contact is labeled '%DB1024.DBX36.3' and is linked to 'F_GLOBDB.VKE0'. The second contact is labeled '%DB1024.DBX36.4' and is linked to 'F_GLOBDB.VKE1'. The network is terminated by a coil labeled '#TEST'.

Le DB global F est un bloc de données de sécurité qui contient toutes les données globales du programme de sécurité ainsi que des informations supplémentaires nécessaires au système F. Le DB global F est inséré automatiquement lors de la compilation de la configuration matérielle.

Via son nom symbolique F_GLOBDB, vous pouvez évaluer certaines données du programme de sécurité dans le programme utilisateur standard.

Vous pouvez, au sein du programme utilisateur standard ou sur un système de contrôle-commande, lire dans le DB global F :

- le mode de fonctionnement mode de sécurité/mode de sécurité désactivé (variable « MODE »)
- l'information d'erreur « Erreur lors du traitement du programme de sécurité » (variable « ERROR »)
- la signature globale F (variable « F_PROG_SIG »)
- la date de compilation du programme de sécurité (variable « F_PROG_DAT », type de donnée DATE AND TIME)

La lecture de ces variables s'effectue par accès entièrement qualifié (par ex. « "F_GLOBDB".MODE »).

6.35.5. Variables du DB de périphérie (300F/400F)

Nom	Type de données	Initialisation	Valeur de défaut	Indicateur de...	Valeur de...	Commentaire
Input						
QAD_I_00	Bool	0.0	True			QAD_I_00: Input 00
QAD_I_01	Bool	0.1	True			QAD_I_01: Input 01
QAD_I_02	Bool	0.2	True			QAD_I_02: Input 02
QAD_I_03	Bool	0.3	True			QAD_I_03: Input 03
Output						
QAD_O_00	Bool	1.0	True			QAD_O_00: Output 00
QAD_O_01	Bool	1.1	True			QAD_O_01: Output 01
QAD_O_02	Bool	1.2	True			QAD_O_02: Output 02
QAD_O_03	Bool	1.3	True			QAD_O_03: Output 03
QAD_I_04	Bool	2.0	True			QAD_I_04: Input 04
QAD_I_05	Bool	2.1	True			QAD_I_05: Input 05
QAD_I_06	Bool	2.2	True			QAD_I_06: Input 06
QAD_I_07	Bool	2.3	True			QAD_I_07: Input 07
QAD_I_08	Bool	2.4	True			QAD_I_08: Input 08
QAD_I_09	Bool	2.5	True			QAD_I_09: Input 09
QAD_I_10	Bool	2.6	True			QAD_I_10: Input 10
QAD_I_11	Bool	2.7	True			QAD_I_11: Input 11
QAD_I_12	Bool	2.8	True			QAD_I_12: Input 12
QAD_I_13	Bool	2.9	True			QAD_I_13: Input 13
QAD_I_14	Bool	3.0	True			QAD_I_14: Input 14
QAD_I_15	Bool	3.1	True			QAD_I_15: Input 15
QAD_I_16	Bool	3.2	True			QAD_I_16: Input 16
QAD_I_17	Bool	3.3	True			QAD_I_17: Input 17
QAD_I_18	Bool	3.4	True			QAD_I_18: Input 18
QAD_I_19	Bool	3.5	True			QAD_I_19: Input 19
QAD_I_20	Bool	3.6	True			QAD_I_20: Input 20
QAD_I_21	Bool	3.7	True			QAD_I_21: Input 21
QAD_I_22	Bool	3.8	True			QAD_I_22: Input 22
QAD_I_23	Bool	3.9	True			QAD_I_23: Input 23
QAD_I_24	Bool	4.0	True			QAD_I_24: Input 24
QAD_I_25	Bool	4.1	True			QAD_I_25: Input 25
QAD_I_26	Bool	4.2	True			QAD_I_26: Input 26
QAD_I_27	Bool	4.3	True			QAD_I_27: Input 27
QAD_I_28	Bool	4.4	True			QAD_I_28: Input 28
QAD_I_29	Bool	4.5	True			QAD_I_29: Input 29
QAD_I_30	Bool	4.6	True			QAD_I_30: Input 30
QAD_I_31	Bool	4.7	True			QAD_I_31: Input 31
QAD_I_32	Bool	4.8	True			QAD_I_32: Input 32
QAD_I_33	Bool	4.9	True			QAD_I_33: Input 33
QAD_I_34	Bool	5.0	True			QAD_I_34: Input 34
QAD_I_35	Bool	5.1	True			QAD_I_35: Input 35
QAD_I_36	Bool	5.2	True			QAD_I_36: Input 36
QAD_I_37	Bool	5.3	True			QAD_I_37: Input 37
QAD_I_38	Bool	5.4	True			QAD_I_38: Input 38
QAD_I_39	Bool	5.5	True			QAD_I_39: Input 39
QAD_I_40	Bool	5.6	True			QAD_I_40: Input 40
QAD_I_41	Bool	5.7	True			QAD_I_41: Input 41
QAD_I_42	Bool	5.8	True			QAD_I_42: Input 42
QAD_I_43	Bool	5.9	True			QAD_I_43: Input 43
QAD_I_44	Bool	6.0	True			QAD_I_44: Input 44
QAD_I_45	Bool	6.1	True			QAD_I_45: Input 45
QAD_I_46	Bool	6.2	True			QAD_I_46: Input 46
QAD_I_47	Bool	6.3	True			QAD_I_47: Input 47
QAD_I_48	Bool	6.4	True			QAD_I_48: Input 48
QAD_I_49	Bool	6.5	True			QAD_I_49: Input 49
QAD_I_50	Bool	6.6	True			QAD_I_50: Input 50
QAD_I_51	Bool	6.7	True			QAD_I_51: Input 51
QAD_I_52	Bool	6.8	True			QAD_I_52: Input 52
QAD_I_53	Bool	6.9	True			QAD_I_53: Input 53
QAD_I_54	Bool	7.0	True			QAD_I_54: Input 54
QAD_I_55	Bool	7.1	True			QAD_I_55: Input 55
QAD_I_56	Bool	7.2	True			QAD_I_56: Input 56
QAD_I_57	Bool	7.3	True			QAD_I_57: Input 57
QAD_I_58	Bool	7.4	True			QAD_I_58: Input 58
QAD_I_59	Bool	7.5	True			QAD_I_59: Input 59
QAD_I_60	Bool	7.6	True			QAD_I_60: Input 60
QAD_I_61	Bool	7.7	True			QAD_I_61: Input 61
QAD_I_62	Bool	7.8	True			QAD_I_62: Input 62
QAD_I_63	Bool	7.9	True			QAD_I_63: Input 63
QAD_I_64	Bool	8.0	True			QAD_I_64: Input 64
QAD_I_65	Bool	8.1	True			QAD_I_65: Input 65
QAD_I_66	Bool	8.2	True			QAD_I_66: Input 66
QAD_I_67	Bool	8.3	True			QAD_I_67: Input 67
QAD_I_68	Bool	8.4	True			QAD_I_68: Input 68
QAD_I_69	Bool	8.5	True			QAD_I_69: Input 69
QAD_I_70	Bool	8.6	True			QAD_I_70: Input 70
QAD_I_71	Bool	8.7	True			QAD_I_71: Input 71
QAD_I_72	Bool	8.8	True			QAD_I_72: Input 72
QAD_I_73	Bool	8.9	True			QAD_I_73: Input 73
QAD_I_74	Bool	9.0	True			QAD_I_74: Input 74
QAD_I_75	Bool	9.1	True			QAD_I_75: Input 75
QAD_I_76	Bool	9.2	True			QAD_I_76: Input 76
QAD_I_77	Bool	9.3	True			QAD_I_77: Input 77
QAD_I_78	Bool	9.4	True			QAD_I_78: Input 78
QAD_I_79	Bool	9.5	True			QAD_I_79: Input 79
QAD_I_80	Bool	9.6	True			QAD_I_80: Input 80
QAD_I_81	Bool	9.7	True			QAD_I_81: Input 81
QAD_I_82	Bool	9.8	True			QAD_I_82: Input 82
QAD_I_83	Bool	9.9	True			QAD_I_83: Input 83
QAD_I_84	Bool	10.0	True			QAD_I_84: Input 84
QAD_I_85	Bool	10.1	True			QAD_I_85: Input 85
QAD_I_86	Bool	10.2	True			QAD_I_86: Input 86
QAD_I_87	Bool	10.3	True			QAD_I_87: Input 87
QAD_I_88	Bool	10.4	True			QAD_I_88: Input 88
QAD_I_89	Bool	10.5	True			QAD_I_89: Input 89
QAD_I_90	Bool	10.6	True			QAD_I_90: Input 90
QAD_I_91	Bool	10.7	True			QAD_I_91: Input 91
QAD_I_92	Bool	10.8	True			QAD_I_92: Input 92
QAD_I_93	Bool	10.9	True			QAD_I_93: Input 93
QAD_I_94	Bool	11.0	True			QAD_I_94: Input 94
QAD_I_95	Bool	11.1	True			QAD_I_95: Input 95
QAD_I_96	Bool	11.2	True			QAD_I_96: Input 96
QAD_I_97	Bool	11.3	True			QAD_I_97: Input 97
QAD_I_98	Bool	11.4	True			QAD_I_98: Input 98
QAD_I_99	Bool	11.5	True			QAD_I_99: Input 99
QAD_I_100	Bool	11.6	True			QAD_I_100: Input 100
QAD_I_101	Bool	11.7	True			QAD_I_101: Input 101
QAD_I_102	Bool	11.8	True			QAD_I_102: Input 102
QAD_I_103	Bool	11.9	True			QAD_I_103: Input 103
QAD_I_104	Bool	12.0	True			QAD_I_104: Input 104
QAD_I_105	Bool	12.1	True			QAD_I_105: Input 105
QAD_I_106	Bool	12.2	True			QAD_I_106: Input 106
QAD_I_107	Bool	12.3	True			QAD_I_107: Input 107
QAD_I_108	Bool	12.4	True			QAD_I_108: Input 108
QAD_I_109	Bool	12.5	True			QAD_I_109: Input 109
QAD_I_110	Bool	12.6	True			QAD_I_110: Input 110
QAD_I_111	Bool	12.7	True			QAD_I_111: Input 111
QAD_I_112	Bool	12.8	True			QAD_I_112: Input 112
QAD_I_113	Bool	12.9	True			QAD_I_113: Input 113
QAD_I_114	Bool	13.0	True			QAD_I_114: Input 114
QAD_I_115	Bool	13.1	True			QAD_I_115: Input 115
QAD_I_116	Bool	13.2	True			QAD_I_116: Input 116
QAD_I_117	Bool	13.3	True			QAD_I_117: Input 117
QAD_I_118	Bool	13.4	True			QAD_I_118: Input 118
QAD_I_119	Bool	13.5	True			QAD_I_119: Input 119
QAD_I_120	Bool	13.6	True			QAD_I_120: Input 120
QAD_I_121	Bool	13.7	True			QAD_I_121: Input 121
QAD_I_122	Bool	13.8	True			QAD_I_122: Input 122
QAD_I_123	Bool	13.9	True			QAD_I_123: Input 123
QAD_I_124	Bool	14.0	True			QAD_I_124: Input 124
QAD_I_125	Bool	14.1	True			QAD_I_125: Input 125
QAD_I_126	Bool	14.2	True			QAD_I_126: Input 126
QAD_I_127	Bool	14.3	True			QAD_I_127: Input 127
QAD_I_128	Bool	14.4	True			QAD_I_128: Input 128
QAD_I_129	Bool	14.5	True			QAD_I_129: Input 129
QAD_I_130	Bool	14.6	True			QAD_I_130: Input 130
QAD_I_131	Bool	14.7	True			QAD_I_131: Input 131
QAD_I_132	Bool	14.8	True			QAD_I_132: Input 132
QAD_I_133	Bool	14.9	True			QAD_I_133: Input 133
QAD_I_134	Bool	15.0	True			QAD_I_134: Input 134
QAD_I_135	Bool	15.1	True			QAD_I_135: Input 135
QAD_I_136	Bool	15.2	True			QAD_I_136: Input 136
QAD_I_137	Bool	15.3	True			QAD_I_137: Input 137
QAD_I_138	Bool	15.4	True			QAD_I_138: Input 138
QAD_I_139	Bool	15.5	True			QAD_I_139: Input 139
QAD_I_140	Bool	15.6	True			QAD_I_140: Input 140
QAD_I_141	Bool	15.7	True			QAD_I_141: Input 141
QAD_I_142	Bool	15.8	True			QAD_I_142: Input 142
QAD_I_143	Bool	15.9	True			QAD_I_143: Input 143
QAD_I_144	Bool	16.0	True			QAD_I_144: Input 144
QAD_I_145	Bool	16.1	True			QAD_I_145: Input 145
QAD_I_146	Bool	16.2	True			QAD_I_146: Input 146
QAD_I_147	Bool	16.3	True			QAD_I_147: Input 147
QAD_I_148	Bool	16.4	True			QAD_I_148: Input 148
QAD_I_149	Bool	16.5	True			QAD_I_149: Input 149
QAD_I_150	Bool	16.6	True			QAD_I_150: Input 150
QAD_I_151	Bool	16.7	True			QAD_I_151: Input 151
QAD_I_152	Bool	16.8	True			QAD_I_152: Input 152
QAD_I_153	Bool	16.9	True			QAD_I_153: Input 153
QAD_I_154	Bool	17.0	True			QAD_I_154: Input 154
QAD_I_155	Bool	17.1	True			QAD_I_155: Input 155
QAD_I_156	Bool	17.2	True			QAD_I_156: Input 156
QAD_I_157	Bool	17.3	True			QAD_I_157: Input 157
QAD_I_158	Bool	17.4	True			QAD_I_158: Input 158
QAD_I_159	Bool	17.5	True			QAD_I_159: Input 159
QAD_I_160	Bool	17.6	True			QAD_I_160: Input 160
QAD_I_161	Bool	17.7	True			QAD_I_161: Input 161
QAD_I_162	Bool	17.8	True			QAD_I_162: Input 162
QAD_I_163	Bool	17.9	True			QAD_I_163: Input 163
QAD_I_164	Bool	18.0	True			QAD_I_164: Input 164
QAD_I_165	Bool	18.1	True			QAD_I_165: Input 165

6.35.6. DB de périphérie de sécurité / Différences lors de l'évaluation (1)

Différences lors de l'évaluation dans S7-1500F et S7-300F/400F

Variables dans le DB de périphérie F ou état de la valeur dans MIE	Périphérie F avec CPU F S7-1500	Périphérie F avec CPU F S7-300/400
ACK_NEC	✓	✓
QBAD	✓	✓
PASS_OUT	✓	✓
QBAD_I_xx *	✗	✓
QBAD_O_xx *	✗	✓
Etat de la valeur	✓	✗

6.35.7. DB de périphérie de sécurité / Différences lors de l'évaluation (2)

Différences lors de l'évaluation dans S7-1500F et S7-300F/400F

Scénario	Etat de la valeur (S7-1500F)	Q_BAD (S7-300F/400F)
Valeur valides sur la périphérie de sécurité (pas d'erreur)	✓	✗
Erreur de canal apparue	✗	✓
Erreur de canal disparue (ACK_REQ)	✗	✓
Acquittement de l'erreur (ACK_REI)	✓	✗

Tables des matières

7.	Communication pour applications de sécurité	7-2
7.1.	Présentation de la communication sécurisée via PROFIBUS DP	7-3
7.2.	Présentation de la communication sécurisée via PROFINET IO	7-4
7.3.	Communication sécurisée CPU-CPU à l'aide d'un coupleur	7-5
7.3.1.	Blocs de communication SENDDP et RCVDP	7-5
7.3.2.	Configuration matérielle du coupleur PN/PN	7-6
7.3.3.	Zones de transfert PN/PN	7-7
7.3.4.	Présentation des blocs SENDDP et RCVDP	7-8
7.3.5.	Paramètres pour SENDDP et RCVDP	7-9
7.3.6.	Adressage de SENDDP et de RCVDP à l'aide d'un ID univoque	7-10
7.3.7.	Paramètre LADDR adressage absolu ou adressage symbolique	7-11
7.4.	PROFINET I-Device	7-12
7.5.	Communication sécurisée I Device - périphérique intelligent	7-13
7.5.1.	Blocs de communication SENDDP et RCVDP	7-13
7.5.1.	Configuration du mode de fonctionnement, affectation et définition des zones de transfert pour I-Device	7-14
7.5.2.	SENDDP, RCVDP et paramètre LADDR	7-15
7.6.	Communication sécurisée avec les systèmes de sécurité	7-16
7.6.1.	SENDDP, RCVDP et paramètre LADDR	7-17
7.7.	Flexible F-Link : principe de communication	7-18
7.8.	Exercice 1 : arrrt d'urgence groupé via un coupleur PN/PN	7-19
7.8.1.	Exercice 1: Configuration et mise en réseau du coupleur PN-PN	7-20
7.8.2.	Exercice 1 : Configurer les zones de transfert du coupleur PN/PN	7-21
7.8.3.	Exercice 1 : Programmer les blocs RCVDP et SENDDP	7-22
7.8.4.	Exercice 1 : Organigramme	7-23
7.9.	Exercice 2 : arrrt d'urgence groupé via I-Device	7-24
7.9.1.	Exercice 2 : Configurer la CPU	7-25
7.10.	Informations	7-26
7.10.1.	Programmation coupleur PN avec firmware v3.0 ou inférieur	7-27
7.10.2.	Exercice 1 : Arrrt d'urgence global via coupleur PN avec firmware V3.0 ou inférieur	7-28
7.10.3.	Informations complémentaires F-Link	7-32

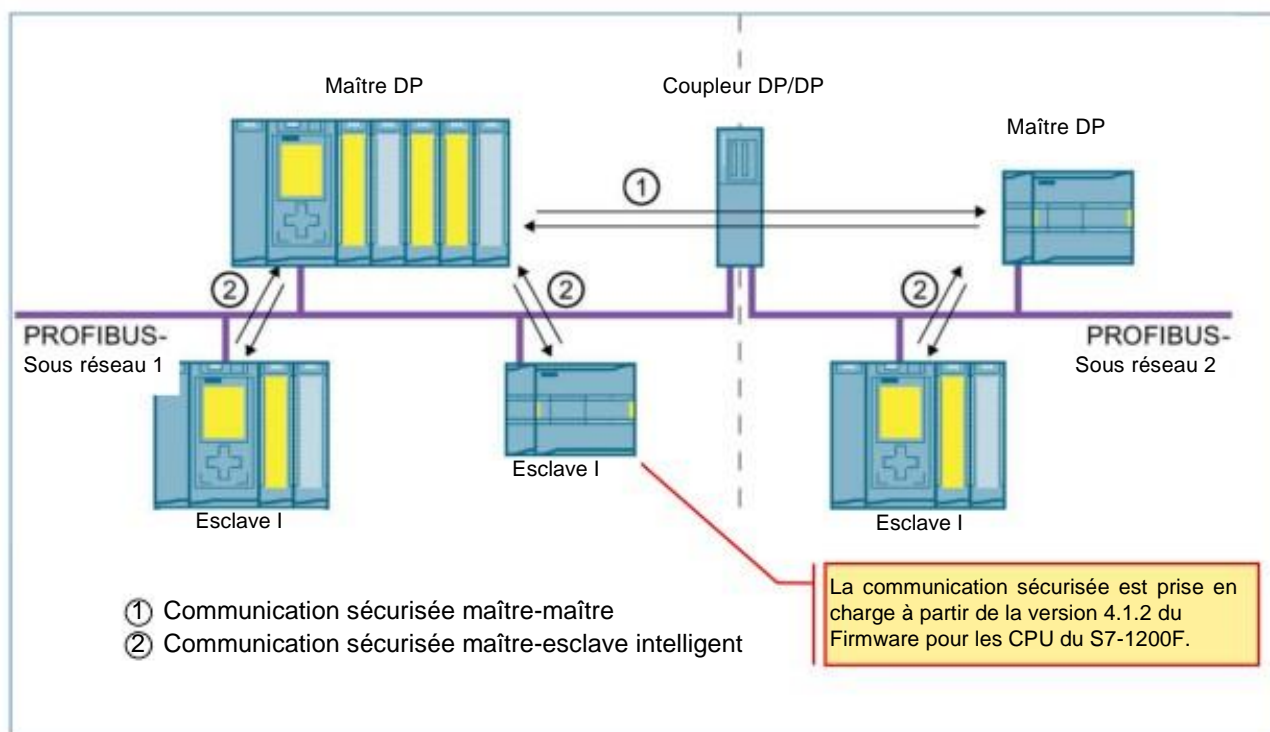
7. Communication pour applications de sécurité

→ l'issue de la formation, le participant au stage ...

- ... aura une vue d'ensemble des différentes possibilités de communication via les réseaux PROFIBUS et PROFINET
- ... pourra expliquer comment fonctionne la communication entre deux CPU à travers un coupleur.
- ... saura configurer et programmer une communication à travers un Contrôleur et un I-Device
- ... sera familiarisé avec la communication flexible F-Link
- ... sera capable d'expliquer comment fonctionne la communication entre des systèmes de sécurité Safety Advanced et Distributed Safety et saura configurer une liaison.



7.1. Présentation de la communication sécurisée via PROFIBUS DP



Communication pour applications de sécurité

PROFIsafe est un protocole de communication sécurisé pour réseaux PROFIBUS ou PROFINET.

PROFIsafe est le premier protocole de communication conforme à la norme de sécurité CEI 61508 qui permet d'échanger des données standard et des données de sécurité sur une seule et même ligne de bus. La combinaison de la communication standard et de la communication sécurisée sur un même réseau représente un potentiel d'économies substantiel, que ce soit pour le câblage comme pour l'installation et la configuration des différents composants du réseau, et facilite grandement la mise à niveau et l'extension des installations existantes.

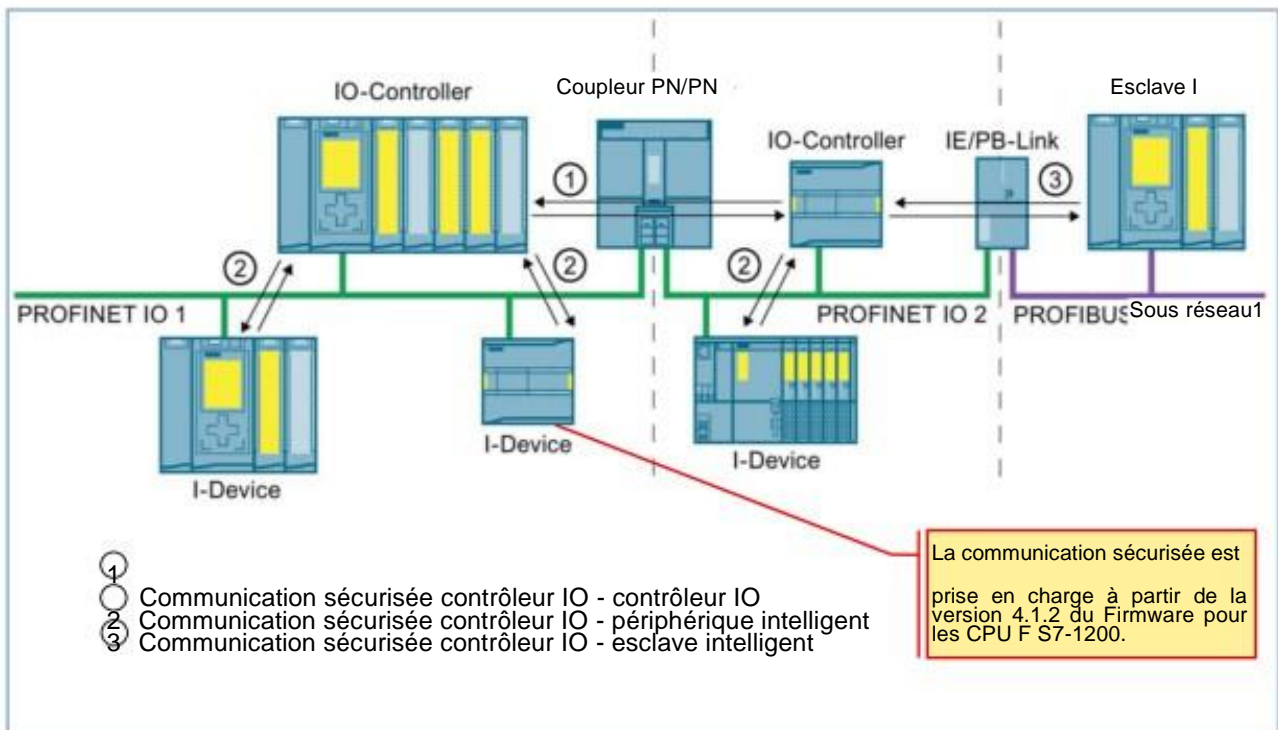
PROFIsafe est une solution ouverte non-propritaire pour bus de terrain standard développée par la communauté des constructeurs d'équipements d'automatisme industriel et des utilisateurs du bus de terrain PROFIBUS, rassemblés au sein de l'association professionnelle PNO.

PROFIsafe sécurise la communication sur les bus ouverts PROFIBUS et PROFINET à partir de composants réseau standard. Combiné au réseau PROFINET, il assure également la communication sécurisée sans fil via IWLAN.

Présentation de la communication sécurisée via PROFIBUS DP

L'illustration ci-dessus présente de manière schématique les possibilités de communication sécurisée sur un réseau PROFIBUS DP (périphérie décentralisée) pour systèmes F SIMATIC Safety dotés de CPU de sécurité S7-1500. Dans une communication sécurisée entre 2 CPU, un volume fixe de données de type BOOL ou INT est échangé entre les programmes de sécurité exécutés sur les CPU F des stations maîtres DP. La transmission s'effectue via l'instruction d'émission SENDDP et l'instruction de réception RCVDP. Les données sont stockées dans des zones de transfert configurées sur chacun des appareils en réseau. Un identifiant matériel (ID matériel) est associé à chacune de ces zones de transfert.

7.2. Présentation de la communication sécurisée via PROFINET IO

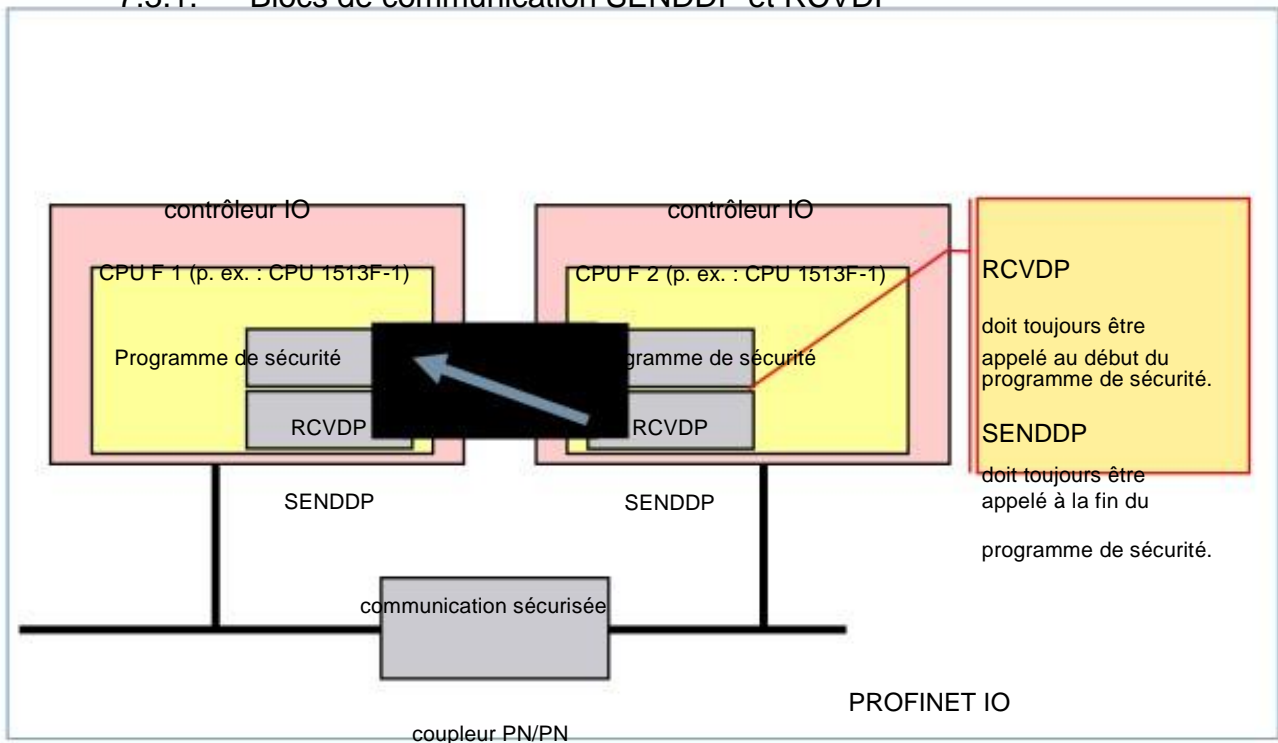


Communication sécurisée entre CPU via PROFINET IO

Dans une communication sécurisée CPU-CPU, un volume fixe de données de type BOOL ou INT est échangé entre les programmes de sécurité exécutés sur les CPU F des contrôleurs IO et des périphériques intelligents décentralisés (I-Device). La transmission s'effectue à l'aide de l'instruction d'émission SENDDP et de l'instruction de réception RCVDP. Les données sont stockées dans des zones de transfert configurées sur les appareils. Un identifiant matériel (ID matériel) est associé à ces zones de transfert.

7.3. Communication sécurisée CPU-CPU à l'aide d'un coupleur

7.3.1. Blocs de communication SENDDP et RCVDP



Configuration de zones de transfert

Des zones de transfert destinées aux données d'entrée et de sortie doivent être configurées dans le coupleur PN/PN. Ces zones sont affectées à l'aide de l'identifiant matériel attribué automatiquement aux modules et aux appareils. Il faut donc connaître l'identifiant matériel pour pouvoir programmer les blocs SENDDP et RCVDP (paramètre LAADR). Pour chaque identifiant matériel associé à une zone de transfert, une constante système est créée dans la CPU F correspondante. Ces constantes peuvent être affectées aux blocs SENDDP et RCVDP selon un mode d'adressage absolu ou symbolique.

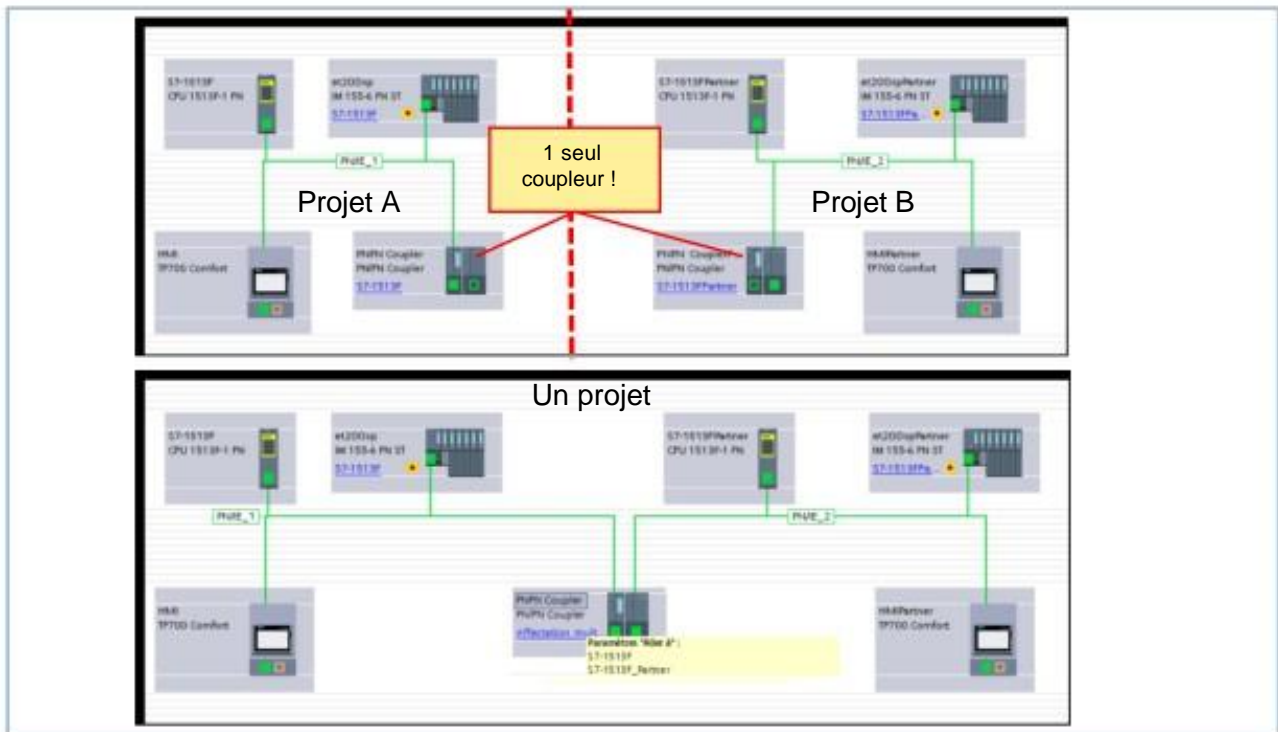
Communication à l'aide des instructions SENDDP et RCVDP

La communication sécurisée entre les CPU F des contrôleurs IO est assurée par l'instruction d'émission SENDDP et l'instruction de réception RCVDP. Ces instructions permettent d'échanger un volume fixe de données sécurisées de type BOOL ou INT (onglet « Instruction » à la rubrique « Communication »).

Remarque

L'instruction RCVDP doit être appelée au début du bloc de sécurité principal (Main Safety). L'instruction SENDDP doit être appelée à la fin du bloc de sécurité principal (Main Safety). Il est à noter que les signaux d'émission ne sont envoyés qu'après l'appel de l'instruction SENDDP, à la fin du traitement du groupe d'exécution de la séquence du programme de sécurité (F-runtime group).

7.3.2. Configuration matérielle du coupleur PN/PN



Remarque

Dans l'éditeur « Appareils et réseaux », désactivez le paramètre d'affichage de validité des données DIA dans les propriétés du coupleur PN/PN. Il s'agit de la configuration par défaut. Si ce paramètre n'est pas désactivé, aucun transfert de données sécurisé ne peut être assuré entre des contrôleurs IO.

Projets distincts

Lorsque les contrôleurs IO qui sont couplés sont programmés dans des projets distincts, il faut insérer le coupleur PN/PN dans les deux projets. Dans les projets il faut affecter l'interface PN respective X1 ou X2 au contrôleur IO. L'interface Pn du partenaire de communication n'est pas à relier ou à affecter.

Projet unique

Lorsque les contrôleurs IO qui seront reliés sont programmés dans un projet commun, il faut programmer le coupleur PN/PN une seule fois. Les interfaces PN X1 ou X2 sont directement affectés aux contrôleurs IO respectifs. Cela fonctionne au mieux avec la fonction Glisser-Déposer d'interface en interface.

7.3.3. Zones de transfert PN/PN

Avec des projets distincts les zones de transfert doivent être renseignées dans les deux projets.

Projet A

Zone de transfert	Emplacement	Type	Longueur I	Longueur Q	Adresse I	Adresse Q	Accès	Dir	Zone de transfert	Emplacement	Type	Longueur I	Longueur Q	Adresse I	Adresse Q	Accès	
Station X1 vers ...	1	IN/OUT	6	12	Byte(s)	100...106	200...211	S7-151BF	Station X1 vers station X2	1	IN/OUT	12	6	Byte(s)	300...312	400...405	S7-151BF
Station X2 vers ...	2	IN/OUT	12	6	Byte(s)	150...163	250...255	S7-151BF	Station X2 vers station X1	2	IN/OUT	6	12	Byte(s)	450...456	450...461	S7-151BF

Projet B

Zone de transfert	Emplacement	Type	Longueur I	Longueur Q	Adresse I	Adresse Q	Accès	Dir	Zone de transfert	Emplacement	Type	Longueur I	Longueur Q	Adresse I	Adresse Q	Accès	
Station X1 vers ...	1	IN/OUT	6	12	Byte(s)	100...106	200...211	S7-151BF	Station X1 vers station X2	1	IN/OUT	12	6	Byte(s)	300...312	400...405	S7-151BF
Station X2 vers ...	2	IN/OUT	12	6	Byte(s)	150...163	250...255	S7-151BF	Station X2 vers station X1	2	IN/OUT	6	12	Byte(s)	450...456	450...461	S7-151BF

SITRAIN © Siemens SAS 2020
Page 7

TIA-SAFETY
Communication SAFETY

Mapping du transfert PROFIsafe

Pour échanger des données avec le coupleur avec PROFIsafe il faut impérativement créer un module de transfert du type « IN/OUT ». La quantité de données est fonction du sens de la communication :

EMISSION : 6 octets IN et 12 octets OUT

RECEPTION : 12 octets IN et 6 octets OUT

Projets distincts

Les deux projets doivent disposer des zones de transfert. Les réglages suivants doivent correspondre : Slot, Type, Longueur I et longueur Q.

Les adresses I et Q peuvent être choisies librement sur chaque CPU.

Les noms des zones de transfert devraient être retenus tout de suite, mais cela n'est pas indispensable.

Projet commun

Les zones de transfert sont programmées en central dans le coupleur. Les réglages des interfaces PN, X1 et X2 sont directement réalisés au niveau du coupleur. Remarque :

- Affectez des noms univoques aux zones de transfert, afin de garantir la lisibilité.
- L'octet d'état des données relatif à la validité des données échangées n'est pas pris en compte car les mécanismes de la communication de sécurité assurent l'intégrité des données utiles. Si l'octet d'état est malgré cela employé alors la version des blocs SENDDP/RCVDP doit être V3.0 ou plus récent.
- Il est recommandé de ne pas utiliser les modules concernés pour d'autres applications.
- Désactivez le paramètre de « validité des données DIA » au niveau des propriétés du coupleur PN/PN. Il s'agit de la configuration par défaut. Si ce paramètre n'est pas désactivé aucune communication de sécurité n'a lieu entre les contrôleurs IO.

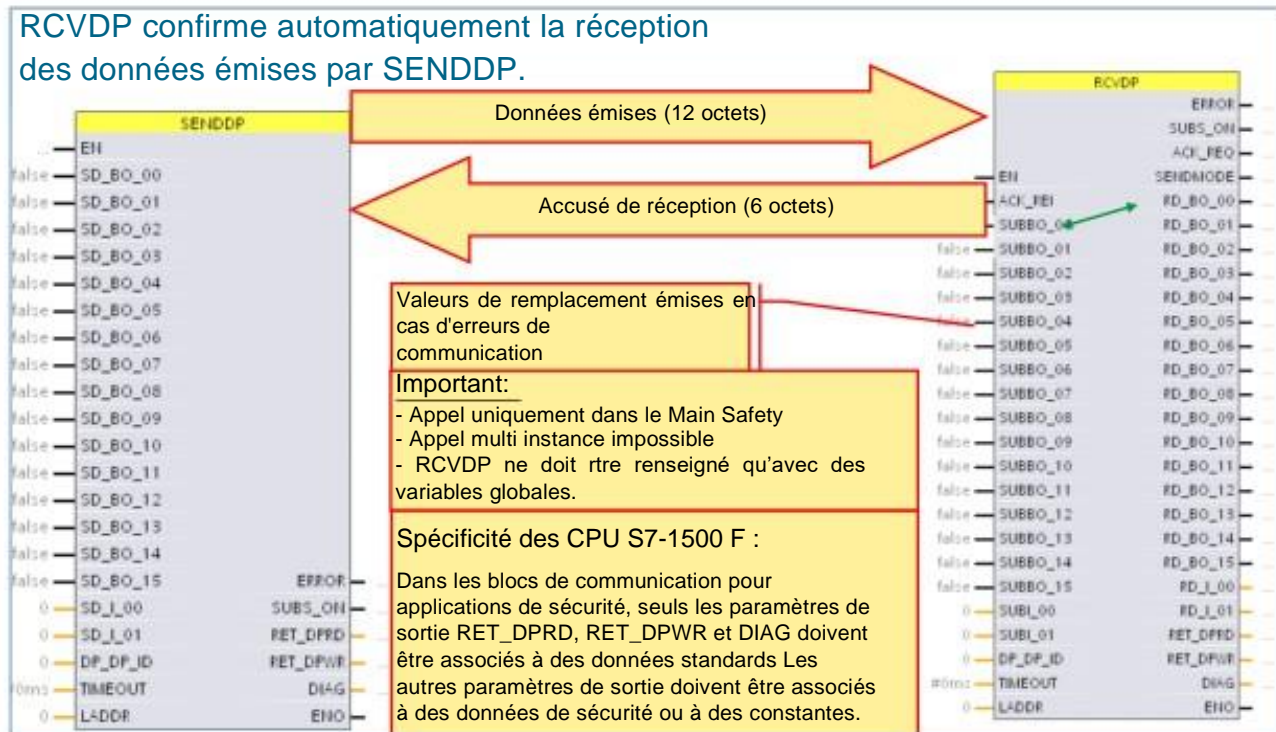
7.3.4. Présentation des blocs SENDDP et RCVDP

- Échange sécurisé de données entre deux programmes de sécurité via un coupleur d'E/S (PROFIBUS + PROFINET)
- Transmission des données assurée par les instructions SENDDP et RCVDP
- Transmission cohérente d'un volume fixe de données
 - 16 valeurs BOOL
 - 2 valeurs INT/1 valeur DINT
 - Paramètres F
 - Paramètres F (acquiescement)
- Stockage des données dans des plages d'adressage configurées
 - Émetteur : 12 octets en sortie 6 octets en entrée
 - Récepteur : 12 octets en entrée 6 octets en sortie

Coupleurs DP/DP et PN/PN

Dans une communication entre deux stations maîtres DP ou entre deux contrôleurs IO, via un module de couplage DP/DP ou PN/PN, le volume fixe de données utiles échangées est de 6 octets. Lors de la configuration des modules dits « universels » intégrés aux coupleurs, vous devez également tenir compte des octets d'entrée et de sortie nécessaires pour la communication sécurisée via le profil PROFIsafe.

7.3.5. Paramètres pour SENDDP et RCVDP



SENDDP et RCVDP

Les données à émettre sont appliquées aux paramètres SD_... dans le bloc SENDDP. Les données reçues sont appliquées aux paramètres RD_... dans le bloc RCVDP. Les valeurs de remplacement générées en cas d'erreur sont appliquées aux paramètres SUB_...

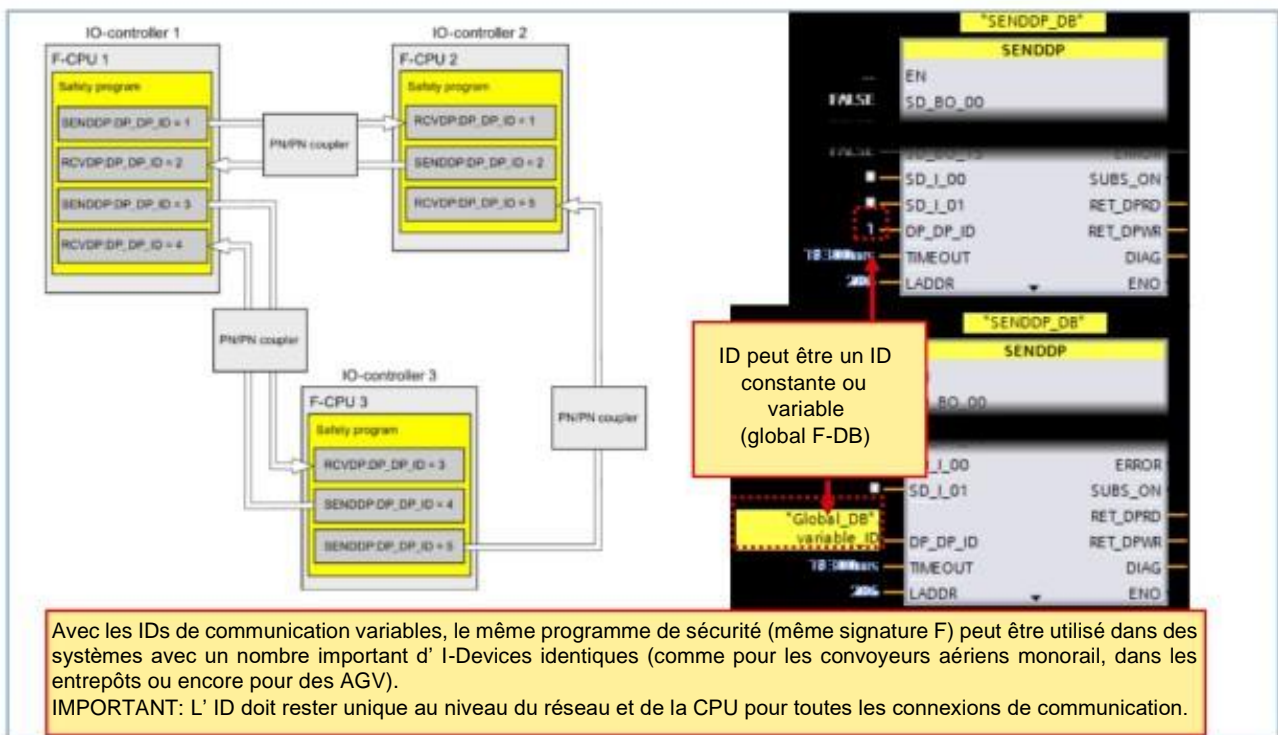
Paramètres d'entrée :

ACK_REI	BOOL	1 = acquittement pour la réintégration des données émises après une erreur de communication
SUBBO_xx	BOOL	valeur de remplacement pour les données reçues BOOL xx (RCVDP seulement)
SUBI_xx	BOOL	valeur de remplacement pour les données reçues INT xx (RCVDP seulement)
SD_BO_xx	BOOL	données émises BOOL xx (SENDDP seulement)
SD_I_xx	INT	données émises INT xx (SENDDP seulement)
DP_DP_ID	INT	identifiant univoque (au choix) dans le réseau pour un binôme SENDDP/RCVDP
TIMEOUT	TIME	temps de surveillance en ms pour la communication sécurisée
LADDR	INT	adresse de l'identifiant matériel (définie dans la configuration de l'appareil)

Paramètres de sortie :

ERROR	BOOL	1 = erreur de communication
SUBS_ON	BOOL	SENDDP : 1 = le récepteur émet des valeurs de remplacement, RCVDP : 1 = des valeurs de remplacement sont émises
ACK_REQ	BOOL	1 = acquittement requis pour la réintégration des données reçues (RCVDP seulement)
SENDMODE	BOOL	1 = CPU F émettrice en mode de sécurité désactivé
RD_BO_xx	BOOL	données reçues BOOL xx
RD_I_xx	INT	données reçues INT xx
RET_DPRD	WORD	code d'erreur
RET_DPWR	WORD	code d'erreur
DIAG	BYTE	données de diagnostic

7.3.6. Adressage de SENDDP et de RCVDP à l'aide d'un ID univoque



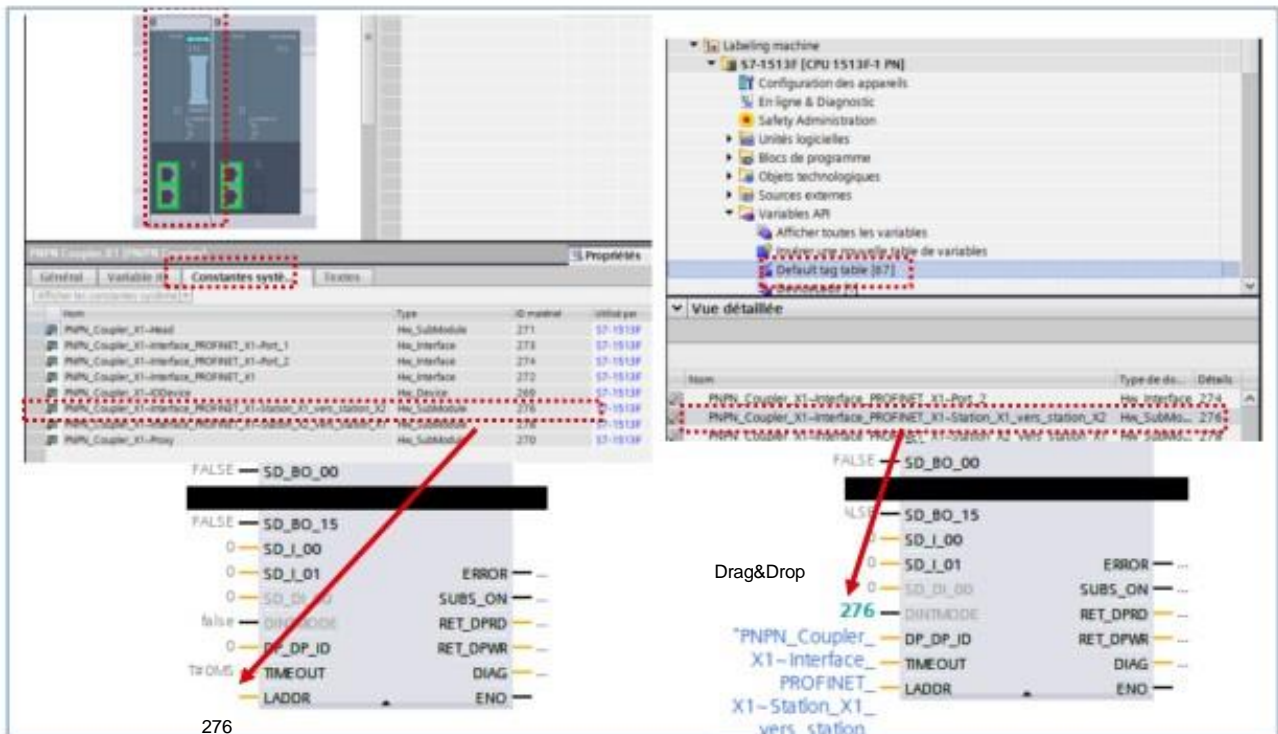
Paramètre DP_DP_ID

Affectez aux entrées DP_DP_ID une valeur d'adressage pour établir la communication entre l'instruction SENDDP d'une CPU F et l'instruction RCVDP d'une autre CPU F. Le paramètre DP_DP_ID doit avoir la même valeur sur les deux instructions concernées.

Remarque

Les valeurs d'adressage (entrée DP_DP_ID, type de données INT) peuvent être définies librement. Toutefois, la valeur d'adressage doit être univoque à l'échelle du réseau pour toutes les liaisons de communication sécurisée. Le caractère univoque de ces valeurs doit être vérifié lors de la réception du programme de sécurité à partir de l'impression du programme de sécurité. Des valeurs constantes doivent être attribuées aux entrées DP_DP_ID et LADDR à l'appel de l'instruction. Le programme de sécurité interdit tout accès direct en lecture ou en écriture aux blocs de données d'instance correspondants.

7.3.7. Paramètre LADDR adressage absolu ou adressage symbolique



Paramètre LADDR en adressage absolu ou symbolique

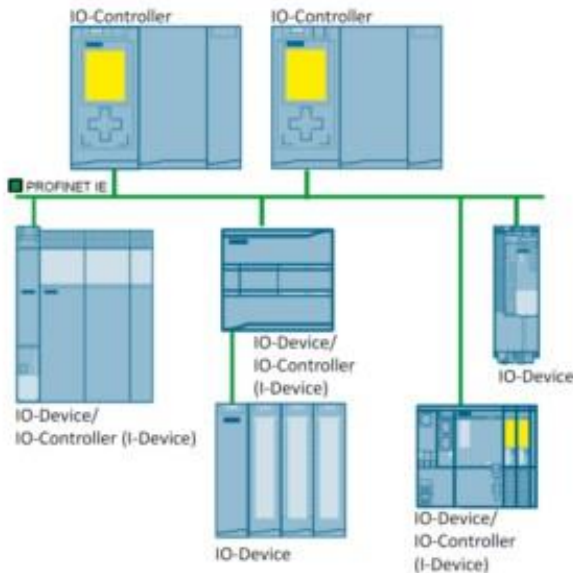
Les zones de transfert sont affectées à l'aide de l'identifiant matériel attribué automatiquement aux modules et aux appareils. Il faut donc connaître l'identifiant matériel pour pouvoir programmer les blocs SENDDP et RCVDP (paramètre LADDR). Pour chaque identifiant matériel associé à une zone de transfert, une constante système est créée dans la CPU F correspondante. Ces constantes peuvent être affectées aux blocs SENDDP et RCVDP selon un mode d'adressage absolu ou symbolique.

Remarque

Si le volume de données à transmettre est supérieur à la capacité disponible sur le binôme d'instructions SENDDP/RCVDP, vous pouvez renouveler l'appel des instructions une seconde fois (voire même une troisième fois). Dans ce cas, configurez une autre liaison de communication via le coupleur PN/PN. En fonction de la limite de capacité du coupleur, cette connexion pourra être établie avec un seul et même coupleur PN/PN.

7.4. PROFINET I-Device

La fonctionnalité « I-Device » (Périphérique IO intelligent) permet à une CPU d'échanger des données avec un contrôleur IO via PROFINET.



- Un contrôleur IO peut être utilisé comme périphérique IO
- Intégration de contrôleurs tiers (GSD)
- Pas de coupleur PN/PN
- Pas d'utilisation de ressources de communication

Propriétés des I-Devices

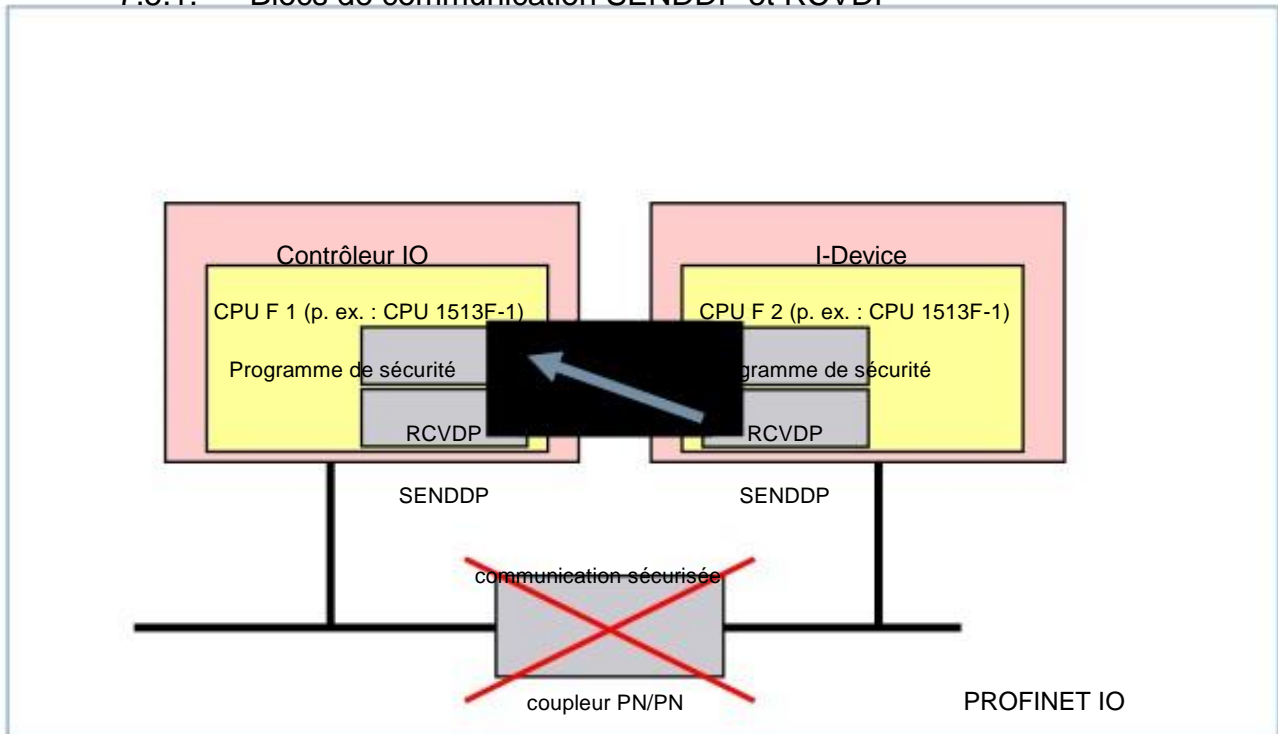
- Découplage de projets STEP 7
Le concepteur et l'utilisateur d'un périphérique intelligent peuvent avoir des projets STEP 7 complètement distincts. Le fichier de description des appareils (GSD) fait le lien entre ces projets. Le couplage à des contrôleurs IO standard est ainsi assuré à travers une interface standardisée.
- Communication en temps réel
Le périphérique intelligent est rattaché à un réseau PROFINET IO déterministe via une interface PROFINET IO. Il prend donc en charge la transmission de données en temps réel (RT) et en temps réel isochrone (IRT).

Avantages du I-Device

- Simplicité de couplage des contrôleurs IO, sans recours à des outils logiciels supplémentaires
- Communication en temps réel entre les CPU SIMATIC et avec les contrôleurs IO standard
- Réduction de la puissance de calcul requise pour chaque CPU, et notamment pour le contrôleur IO, grâce à la répartition de la charge de calcul sur plusieurs I-Device
- Réduction de la charge de communication grâce au traitement sur site des données de process
- Meilleure visibilité grâce à la segmentation du traitement des tâches dans des projets STEP 7 distincts

7.5. Communication sécurisée I Device - périphérique intelligent

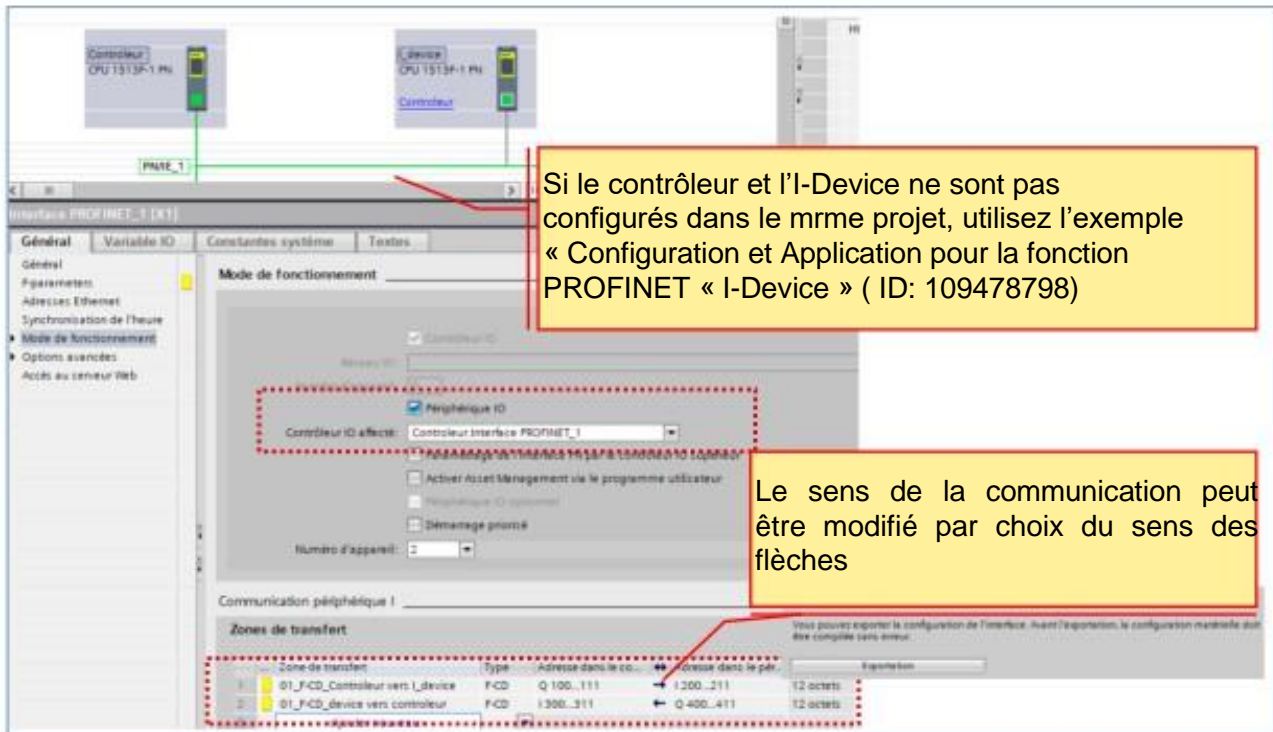
7.5.1. Blocs de communication SENDDP et RCVDP



Périphérique intelligent (I-Device)

Au sein d'une solution d'automatisation classique avec plusieurs automates en réseau, la fonction I-Device permet d'utiliser une CPU aussi bien comme contrôleur IO que comme périphérique IO. Elle peut ainsi communiquer non seulement avec un réseau subordonné, mais aussi avec des contrôleurs IO de niveau supérieur ou des périphéries centralisées, via PROFINET. Ces échanges de données se font simultanément, sur le même bus. La topologie du système est plus légère et plus flexible. Il est ainsi plus facile d'interconnecter des automates issus de projets différents, ou encore d'intégrer des automates Siemens et des automates tiers dans un même réseau de communication.

7.5.1. Configuration du mode de fonctionnement, affectation et définition des zones de transfert pour I-Device



Communication de sécurité contrôleur IO - I-Device

La communication sécurisée entre un contrôleur IO et un ou plusieurs I-Devices est assurée par une liaison entre les programmes de sécurité des CPU F concernées, comme dans une communication classique via PROFINET IO à l'aide de liaisons IO-Contrôleur -I-Device (F-CD). Aucune composante matérielle supplémentaire n'est nécessaire.

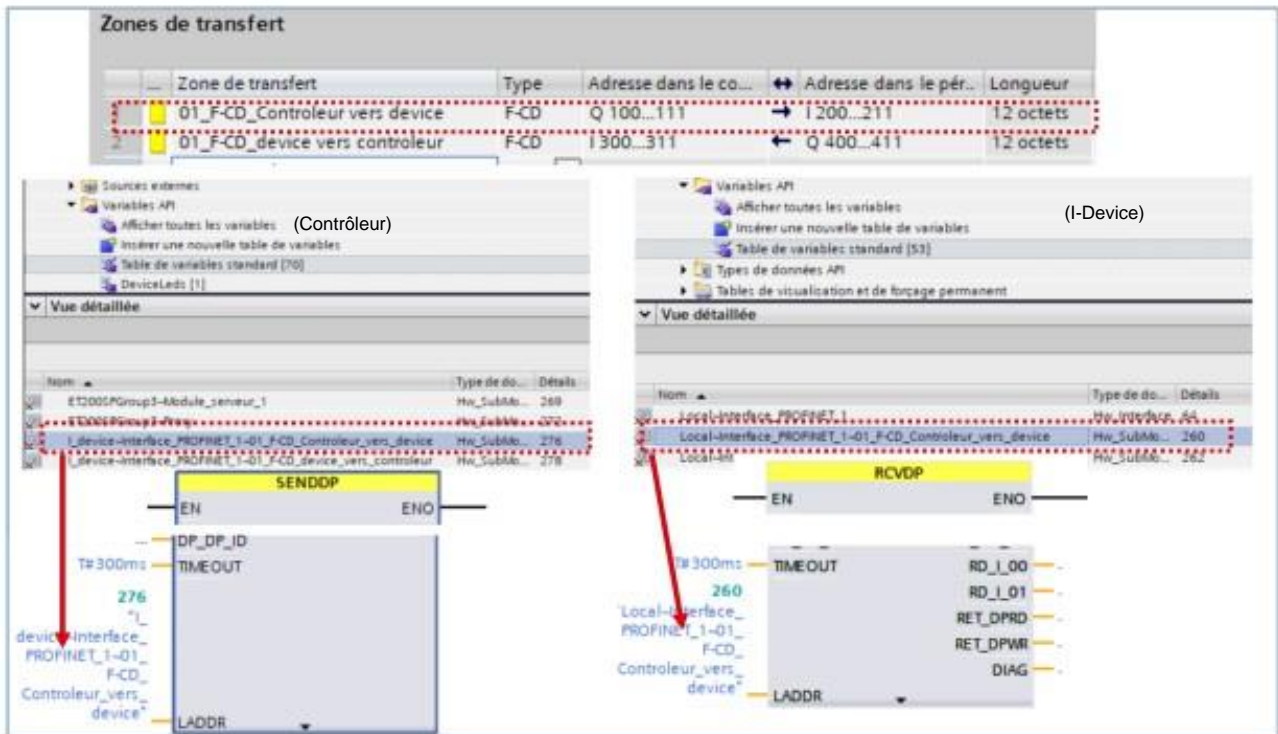
Mode de fonctionnement et affectation d'un périphérique intelligent à un contrôleur IO

Dans les propriétés du contrôleur, cochez l'option IO Device, puis affectez-lui un contrôleur IO.

Configuration des zones de transfert

Pour chaque connexion de communication sécurisée entre deux CPU F, vous devez configurer des zones de transfert dans l'éditeur « Appareils et réseaux ». Lorsqu'une zone de transfert est créée, un code permettant d'identifier la liaison de communication correspondante lui est attribué. Par exemple, « F-CD_PLC_2-PLC_1_1 » indique une connexion F-CD établie entre l'IO contrôleur CPU 1 et le I-DeviceF-CPU2. D'autre part, des constantes système portant le nom de la zone sont créées dans la CPU F du contrôleur IO et dans celle I Device. Ces constantes système contiennent l'identifiant matériel de la zone de transfert propre à chaque CPU F. Enfin, pour chaque liaison F-CD, une liaison destinée à l'envoi d'un accusé de réception est créée automatiquement.

7.5.2. SENDDP, RCVDP et paramètre LADDR



Paramètre LADDR

Affectez les identifiants matériels (constantes système répertoriées dans les tables de variables standard) des zones de transfert dans les programmes de sécurité au paramètre LADDR des instructions SENDDP et RCVDP, selon un mode d'adressage symbolique.

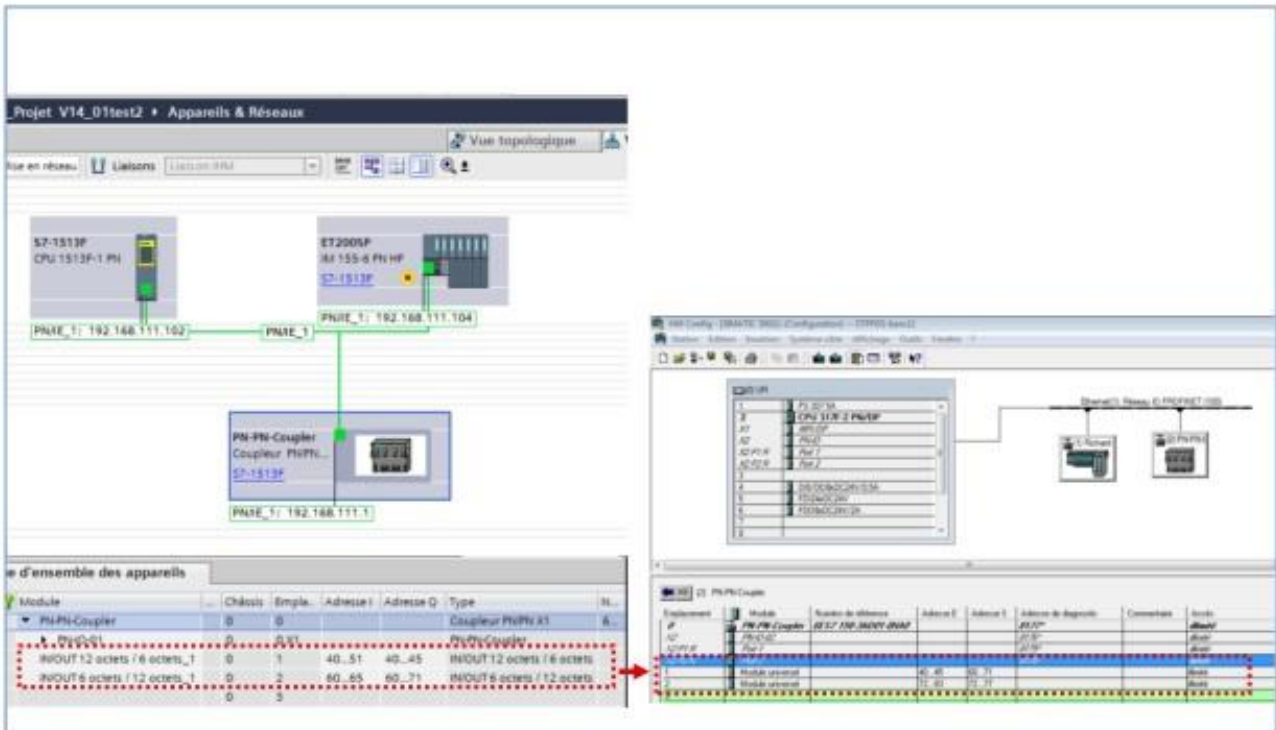
Communication à l'aide des instructions SENDDP et RCVDP

La communication sécurisée entre l'IO Contrôleur et le IDevice est également assurée par l'instruction d'émission SENDDP et l'instruction de réception RCVDP. Ces instructions permettent d'échanger un volume fixe de données sécurisées de type BOOL ou INT. Vous trouvez ces instructions au niveau de la barre des tâches « Instruction », rubrique « Communication »).

Remarque

Si le volume de données à transmettre est supérieur à la capacité disponible pour le binôme d'instructions SENDDP/RCVDP, vous pouvez recourir à des instructions SENDDP/RCVDP supplémentaires. Pour cela, configurez d'autres zones de transfert. Lorsque les données sont transmises entre un périphérique I et un contrôleur IO, la limite maximale à respecter est de 1 440 octets en entrée et 1 440 octets en sortie. Cette limite prend en compte toutes les connexions de communication standard et sécurisées qui ont été configurées (zones de transfert de type CD et F-CD). De plus, une partie de ce volume est utilisé à des fins internes, de sorte que la limite maximale peut être atteinte rapidement. Si elle est dépassée, un message d'erreur est émis.

7.6. Communication sécurisée avec les systèmes de sécurité



Communication sécurisée avec les systèmes de sécurité S7

La communication entre les CPU de sécurité dans SIMATIC Safety et les CPU de sécurité dans les systèmes S7 Distributed Safety peut être assurée à l'aide d'un coupleur PN/PN ou DP/DP. Elle peut donc prendre la forme d'une communication contrôleur IO - contrôleur IO ou maître-maître.

Communication avec S7 Distributed Safety

La communication utilise les instructions SENDDP et RCVDP dans STEP 7 Safety Advanced V1x et les blocs d'application de sécurité SENDDP et RCVDP dans S7 Distributed Safety.

7.6.1. SENDDP, RCVDP et paramètre LADDR

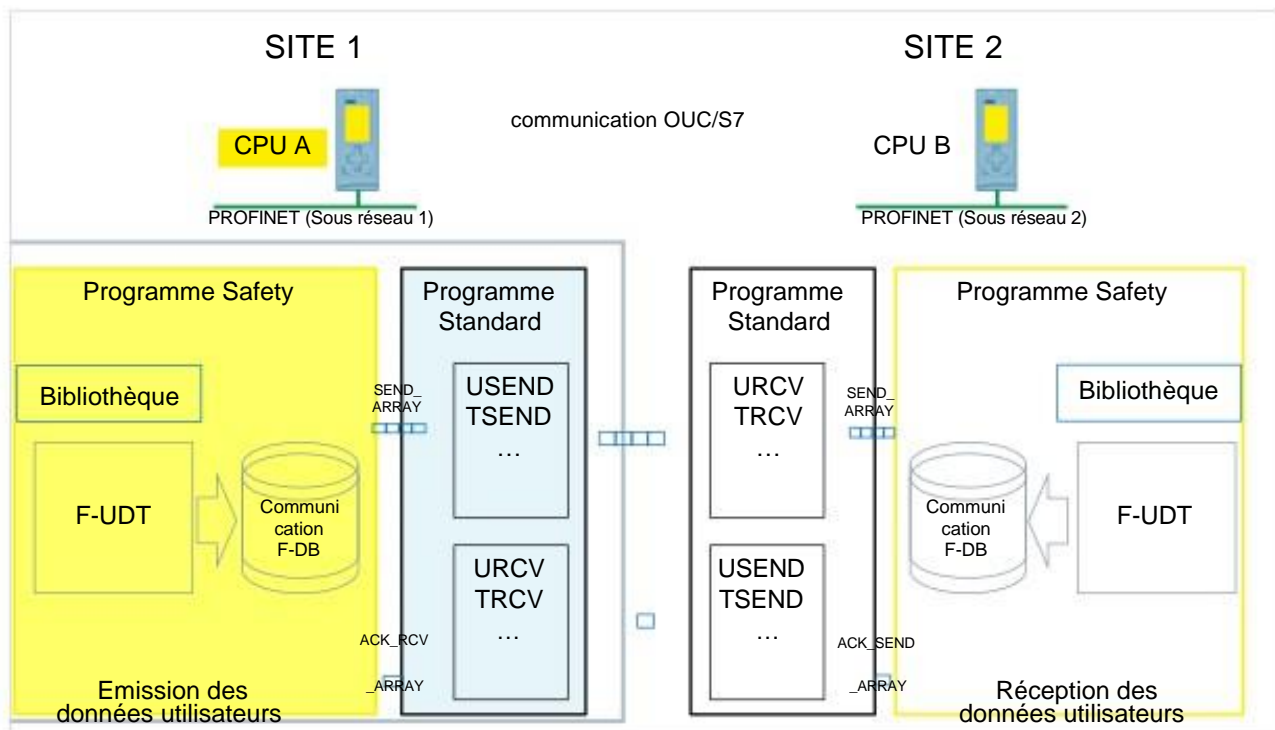
The screenshot displays the SIMATIC Manager interface. On the left, the 'Project Explorer' shows the project structure. The main window shows the 'SENDDP' function block configuration. The 'EN' input is set to 'FALSE'. The 'SD' inputs are set to 'SD_00' through 'SD_15'. The 'DI' inputs are set to 'DI_00' through 'DI_15'. The 'DO' outputs are set to 'DO_00' through 'DO_15'. The 'LADDR' parameter is set to '72'. The 'LADDR' parameter is highlighted with a red arrow. The 'LADDR' parameter is also shown in the 'Hardware Catalog' table below.

Emplacement	Module	Numéro de référence	Adresse I	Adresse S	Adresse de
0	PS 307 5A0	6ES7 307-1EA00-0AA0			0
1	PS 307 5A0	6ES7 307-1EA00-0AA0			1
2	PS 307 5A0	6ES7 307-1EA00-0AA0			2
3	PS 307 5A0	6ES7 307-1EA00-0AA0			3
4	PS 307 5A0	6ES7 307-1EA00-0AA0			4
5	PS 307 5A0	6ES7 307-1EA00-0AA0			5
6	PS 307 5A0	6ES7 307-1EA00-0AA0			6
7	PS 307 5A0	6ES7 307-1EA00-0AA0			7
8	PS 307 5A0	6ES7 307-1EA00-0AA0			8
9	PS 307 5A0	6ES7 307-1EA00-0AA0			9
10	PS 307 5A0	6ES7 307-1EA00-0AA0			10
11	PS 307 5A0	6ES7 307-1EA00-0AA0			11
12	PS 307 5A0	6ES7 307-1EA00-0AA0			12
13	PS 307 5A0	6ES7 307-1EA00-0AA0			13
14	PS 307 5A0	6ES7 307-1EA00-0AA0			14
15	PS 307 5A0	6ES7 307-1EA00-0AA0			15
16	PS 307 5A0	6ES7 307-1EA00-0AA0			16
17	PS 307 5A0	6ES7 307-1EA00-0AA0			17
18	PS 307 5A0	6ES7 307-1EA00-0AA0			18
19	PS 307 5A0	6ES7 307-1EA00-0AA0			19
20	PS 307 5A0	6ES7 307-1EA00-0AA0			20
21	PS 307 5A0	6ES7 307-1EA00-0AA0			21
22	PS 307 5A0	6ES7 307-1EA00-0AA0			22
23	PS 307 5A0	6ES7 307-1EA00-0AA0			23
24	PS 307 5A0	6ES7 307-1EA00-0AA0			24
25	PS 307 5A0	6ES7 307-1EA00-0AA0			25
26	PS 307 5A0	6ES7 307-1EA00-0AA0			26
27	PS 307 5A0	6ES7 307-1EA00-0AA0			27
28	PS 307 5A0	6ES7 307-1EA00-0AA0			28
29	PS 307 5A0	6ES7 307-1EA00-0AA0			29
30	PS 307 5A0	6ES7 307-1EA00-0AA0			30
31	PS 307 5A0	6ES7 307-1EA00-0AA0			31
32	PS 307 5A0	6ES7 307-1EA00-0AA0			32
33	PS 307 5A0	6ES7 307-1EA00-0AA0			33
34	PS 307 5A0	6ES7 307-1EA00-0AA0			34
35	PS 307 5A0	6ES7 307-1EA00-0AA0			35
36	PS 307 5A0	6ES7 307-1EA00-0AA0			36
37	PS 307 5A0	6ES7 307-1EA00-0AA0			37
38	PS 307 5A0	6ES7 307-1EA00-0AA0			38
39	PS 307 5A0	6ES7 307-1EA00-0AA0			39
40	PS 307 5A0	6ES7 307-1EA00-0AA0			40
41	PS 307 5A0	6ES7 307-1EA00-0AA0			41
42	PS 307 5A0	6ES7 307-1EA00-0AA0			42
43	PS 307 5A0	6ES7 307-1EA00-0AA0			43
44	PS 307 5A0	6ES7 307-1EA00-0AA0			44
45	PS 307 5A0	6ES7 307-1EA00-0AA0			45
46	PS 307 5A0	6ES7 307-1EA00-0AA0			46
47	PS 307 5A0	6ES7 307-1EA00-0AA0			47
48	PS 307 5A0	6ES7 307-1EA00-0AA0			48
49	PS 307 5A0	6ES7 307-1EA00-0AA0			49
50	PS 307 5A0	6ES7 307-1EA00-0AA0			50
51	PS 307 5A0	6ES7 307-1EA00-0AA0			51
52	PS 307 5A0	6ES7 307-1EA00-0AA0			52
53	PS 307 5A0	6ES7 307-1EA00-0AA0			53
54	PS 307 5A0	6ES7 307-1EA00-0AA0			54
55	PS 307 5A0	6ES7 307-1EA00-0AA0			55
56	PS 307 5A0	6ES7 307-1EA00-0AA0			56
57	PS 307 5A0	6ES7 307-1EA00-0AA0			57
58	PS 307 5A0	6ES7 307-1EA00-0AA0			58
59	PS 307 5A0	6ES7 307-1EA00-0AA0			59
60	PS 307 5A0	6ES7 307-1EA00-0AA0			60
61	PS 307 5A0	6ES7 307-1EA00-0AA0			61
62	PS 307 5A0	6ES7 307-1EA00-0AA0			62
63	PS 307 5A0	6ES7 307-1EA00-0AA0			63
64	PS 307 5A0	6ES7 307-1EA00-0AA0			64
65	PS 307 5A0	6ES7 307-1EA00-0AA0			65
66	PS 307 5A0	6ES7 307-1EA00-0AA0			66
67	PS 307 5A0	6ES7 307-1EA00-0AA0			67
68	PS 307 5A0	6ES7 307-1EA00-0AA0			68
69	PS 307 5A0	6ES7 307-1EA00-0AA0			69
70	PS 307 5A0	6ES7 307-1EA00-0AA0			70
71	PS 307 5A0	6ES7 307-1EA00-0AA0			71
72	PS 307 5A0	6ES7 307-1EA00-0AA0			72
73	PS 307 5A0	6ES7 307-1EA00-0AA0			73
74	PS 307 5A0	6ES7 307-1EA00-0AA0			74
75	PS 307 5A0	6ES7 307-1EA00-0AA0			75
76	PS 307 5A0	6ES7 307-1EA00-0AA0			76
77	PS 307 5A0	6ES7 307-1EA00-0AA0			77
78	PS 307 5A0	6ES7 307-1EA00-0AA0			78
79	PS 307 5A0	6ES7 307-1EA00-0AA0			79
80	PS 307 5A0	6ES7 307-1EA00-0AA0			80
81	PS 307 5A0	6ES7 307-1EA00-0AA0			81
82	PS 307 5A0	6ES7 307-1EA00-0AA0			82
83	PS 307 5A0	6ES7 307-1EA00-0AA0			83
84	PS 307 5A0	6ES7 307-1EA00-0AA0			84
85	PS 307 5A0	6ES7 307-1EA00-0AA0			85
86	PS 307 5A0	6ES7 307-1EA00-0AA0			86
87	PS 307 5A0	6ES7 307-1EA00-0AA0			87
88	PS 307 5A0	6ES7 307-1EA00-0AA0			88
89	PS 307 5A0	6ES7 307-1EA00-0AA0			89
90	PS 307 5A0	6ES7 307-1EA00-0AA0			90
91	PS 307 5A0	6ES7 307-1EA00-0AA0			91
92	PS 307 5A0	6ES7 307-1EA00-0AA0			92
93	PS 307 5A0	6ES7 307-1EA00-0AA0			93
94	PS 307 5A0	6ES7 307-1EA00-0AA0			94
95	PS 307 5A0	6ES7 307-1EA00-0AA0			95
96	PS 307 5A0	6ES7 307-1EA00-0AA0			96
97	PS 307 5A0	6ES7 307-1EA00-0AA0			97
98	PS 307 5A0	6ES7 307-1EA00-0AA0			98
99	PS 307 5A0	6ES7 307-1EA00-0AA0			99

SENDDP, RCVDP et paramètre LADDR

Pour programmer une CPU S7-300 ou S7-400 F, utilisez les adresses de début des zones de transfert. Pour programmer une CPU S7-1500 F, utilisez les identifiants matériels des zones de transfert.

7.7. Flexible F-Link : principe de communication



Généralités

Pour les CPUs S7-1200/1500 F vous disposez d'une nouvelle communication CPU-CPU « Flexible F-Link ». Les données de sécurité peuvent ainsi être échangées entre des CPU F à l'aide de UDT F à l'aide de mécanisme de communication standard.

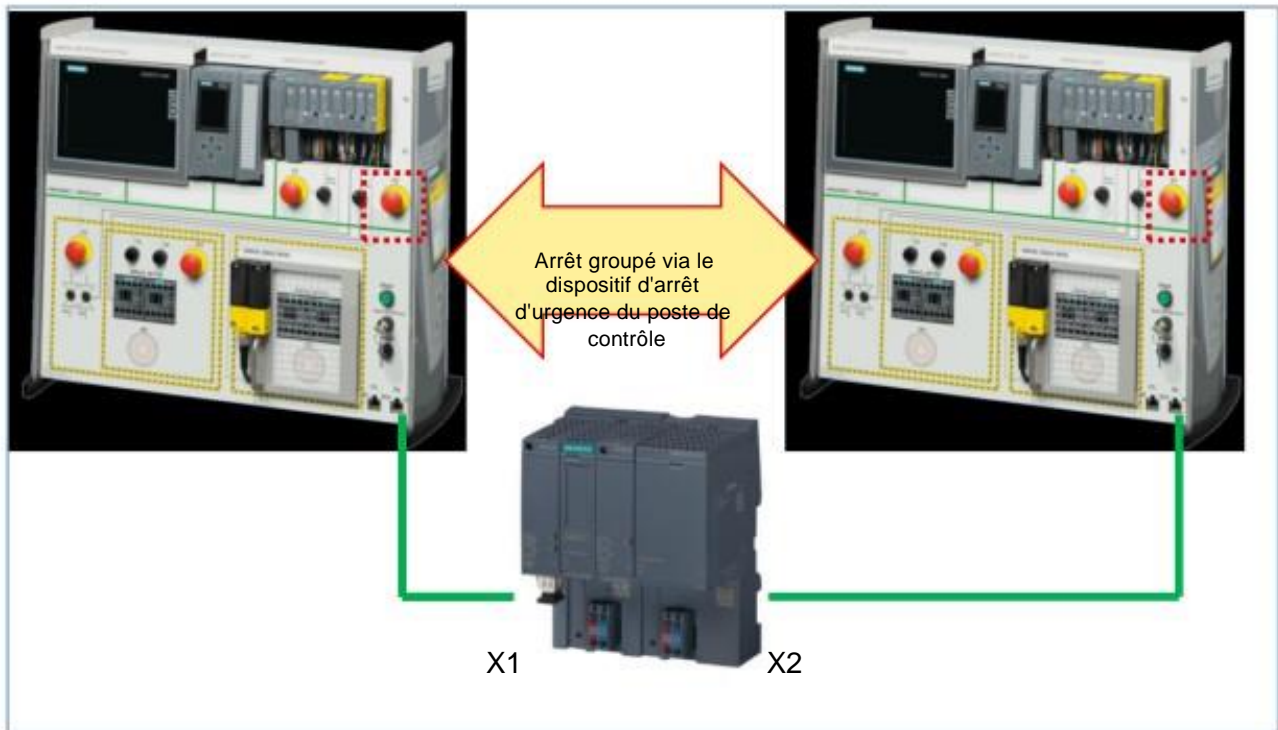
Avantage

- Compactage des données de sécurité à transmettre sous forme de type de données API F
- Jusqu'à 100 octets de données de sécurité
- Supporte les types de données de sécurité
- Paramétrage simple et génération automatique de DB de communication de sécurité
- Transfert de données de sécurité à l'aide blocs de communication standard même au-delà des limites du réseau
- Communication entre groupe d'exécution F pour CPU S7-1200/1500 F
- UUID (Identifiant Universel Unique) de Communication F : univoque, intégrée au système et universelle
- Signature individuelle des adresses de communication F pour la reconnaissance simple des modifications des UUID pour communications F

Conditions

- S7-1200 F-CPU à partir de Firmware V4.2
- S7-1500 F-CPU à partir de Firmware V2.0
- Version système safety V2.2 ou supérieure

7.8. Exercice 1 : arrêt d'urgence groupé via un coupleur PN/PN



Enoncé

Actuellement chaque station travaille séparément sans liaison aux autres stations. Il faut maintenant réaliser une communication sûre entre 2 stations. La communication doit être réalisée via un coupleur PN/PN. Il doit être maintenant possible de désactiver la station partenaire via un arrêt d'urgence et inversement.

Préparation

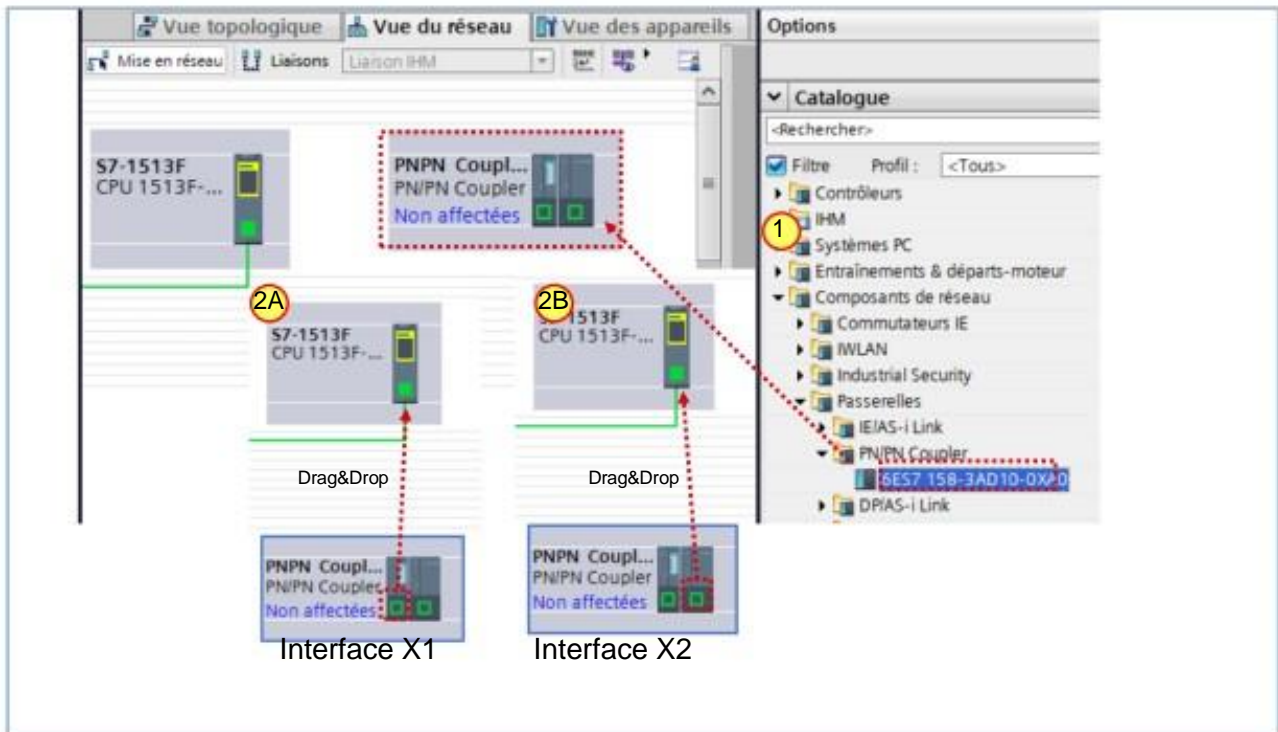
1. Choisissez avec votre groupe partenaire le coupleur utilisé ainsi que les interfaces X1 ou X2 utilisées.
La station / groupe, qui utilise l'interface du coupleur X1 (gauche), travaille par la suite les étapes marquées par. **A**

Par analogie, la station/groupe qui utilise l'interface coupleur X2 (droite) travaille avec les étapes marquées par. **B**

2. Connectez votre station et le coupleur via PROFINET.

Suite page suivante


7.8.1. Exercice 1: Configuration et mise en réseau du coupleur PN-PN




Marche à suivre

1. Copier avec Glisser-Déposer le coupleur PN/PN à partir du catalogue matériel

« Profinet IO > Passerelle > Coupleur PN/PN » dans la vue du réseau.

 Affecter l'interface du coupleur X1 (gauche) par Glisser - Déposer à votre CPU et adaptez le nom de l'appareil et l'adresse IP (Cf. feuille descriptive dans coffret).

 Affecter l'interface du coupleur X21 (droite) par Glisser - Déposer à votre CPU et adaptez le nom de l'appareil et l'adresse IP (Cf. feuille descriptive dans coffret).

Suite page suivante

7.8.2. Exercice 1 : Configurer les zones de transfert du coupleur PN/PN



1. Ouvrez dans les propriétés du coupleur « Transferring ».
 Insérez deux zones de transfert pour l'émission et la réception des données PROFI-safe.
 Renseignez les paramètres des zones de transfert de l'interface PROFINET X1 comme indiqué

2. Ouvrez les propriétés du coupleur « Transferring ».
 Insérez deux zones de transfert pour l'émission et la réception des données PROFI-safe.
 Renseignez les paramètres des zones de transfert de l'interface PROFINET X1 comme indiqué

- Affectez un nom d'appareil en ligne au coupleur PN/PN.
- Enregistrez et chargez votre projet

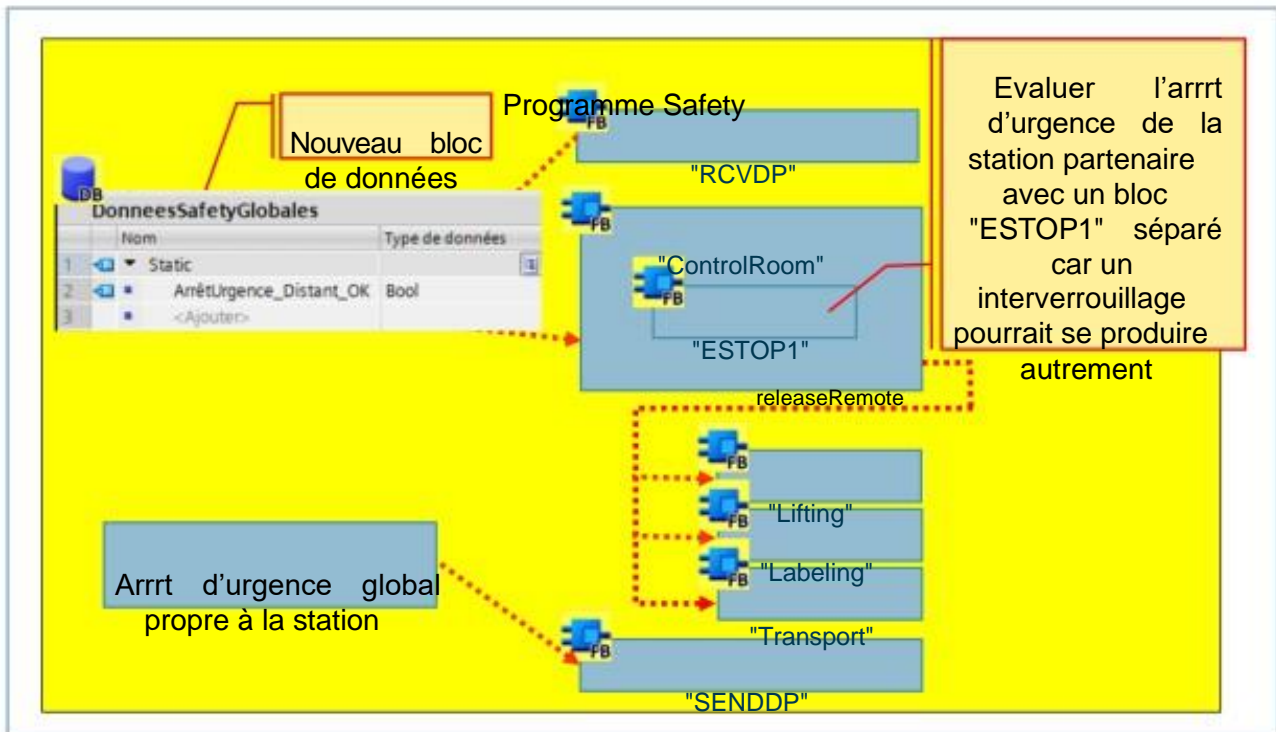
Résultat :

Le système entier devrait démarrer sans erreur une fois la station partenaire également chargée.

Si ce n'est pas le cas, contrôlez une nouvelle fois le paramétrage et la liaison du coupleur PN/PN (Les deux groupes !)

Suite page suivante

7.8.3. Exercice 1 : Programmer les blocs RCVDP et SENDDP



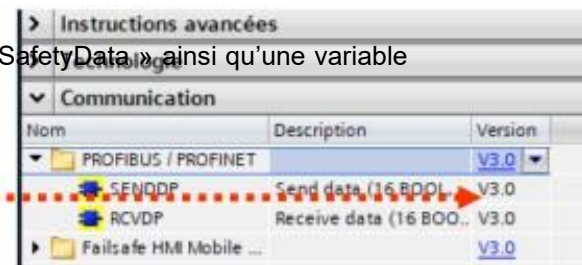
1. Créez un bloc de données global de sécurité « GlobalSafetyData » ainsi qu'une variable (Bool) "remoteEstopOK".
2. Appelez le bloc d'émission « SENDDP » et le bloc de réception « RCVDP » au bon endroit de votre programme de sécurité.

Remarque : Utilisez la version la plus récente des blocs !

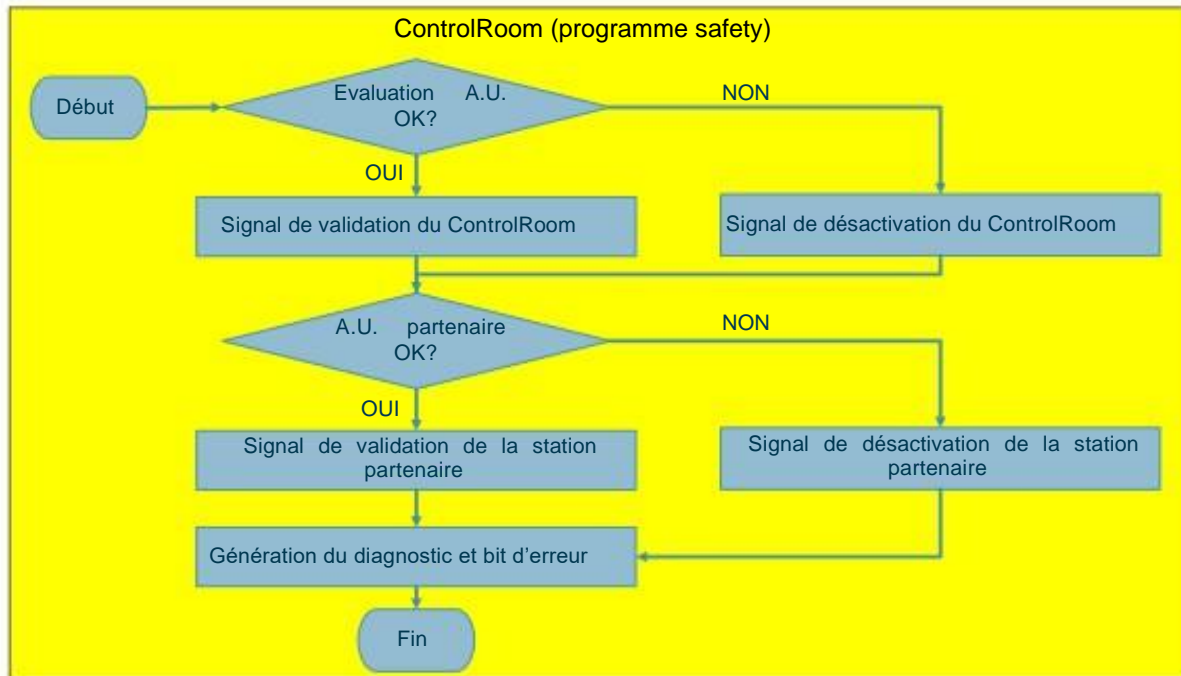
- Transférez la libération globale de l'arrêt d'urgence (E2) via le bloc d'émission « SENDDP » à la station partenaire.
- Sauvegardez la libération de l'arrêt d'urgence de la station partenaire dans la station partenaire "GlobalSafetyData".remoteEstopOk.
- Paramétrez les autres interfaces nécessaires du bloc de données d'émission et de réception en fonction de la configuration de votre coupleur.

Remarque : il faut se synchroniser avec le groupe partenaire

Suite page suivante



7.8.4. Exercice 1 : Organigramme



11. Le signal de validation global de la station partenaire ("GlobalSafetyData".remoteEstopOk) doit maintenant être exploité par tous les appareils de l'installation. Évaluez dans le bloc de sécurité « ControlRoom » l'arrêt d'urgence rajouté par un nouvel appel de ESTOP1 »

Note : Si l'évaluation est intégrée dans le bloc « ESTOP1 » existant il en résultera un interverrouillage.

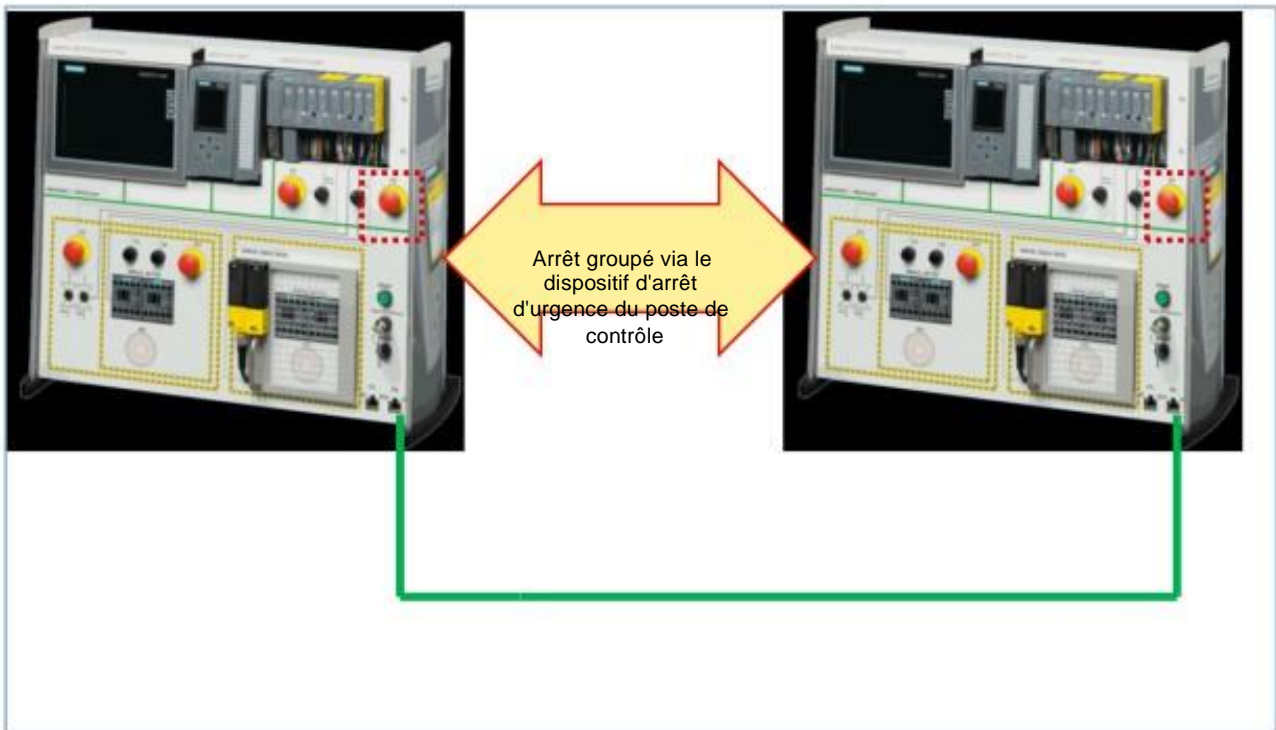
12. Transmettre le signal d'arrêt global nouvellement généré à toutes les unités. La fonctionnalité est identique à celle de l'arrêt d'urgence global existant.
13. Chargez tous les blocs dans la CPU.
14. Enregistrez votre projet et testez la fonction.

Résultat :

Les deux stations doivent pouvoir désormais placer l'installation commandée par la station partenaire à l'état de sécurité (coupure de l'installation) via le bouton d'arrêt d'urgence (E2) du poste de contrôle.

Remarque: Lors de la coupure par la station partenaire il faut d'abord acquitter la station partenaire puis la station elle-même

7.9. Exercice 2 : arrêt d'urgence groupé via I-Device



Énoncé

La communication sécurisée via un coupleur PN/PN doit maintenant être remplacée par une communication sécurisée via I-Device. La possibilité de désactiver une station partenaire à l'aide du bouton d'arrêt d'urgence de la station Poste de contrôle doit être maintenue, la station partenaire doit posséder la même possibilité.

Procédure

1. Établissez une connexion PROFINET directe avec la CPU de la station partenaire et clarifier quel groupe prend le rôle du groupe IO Contrôleur et quel groupe prend le rôle de l'I-Device.
2. Pour la programmation vous utiliserez l'exemple applicatif

« Communication de sécurité IO-Controller-I-Device » Vous trouvez le document sur votre PC

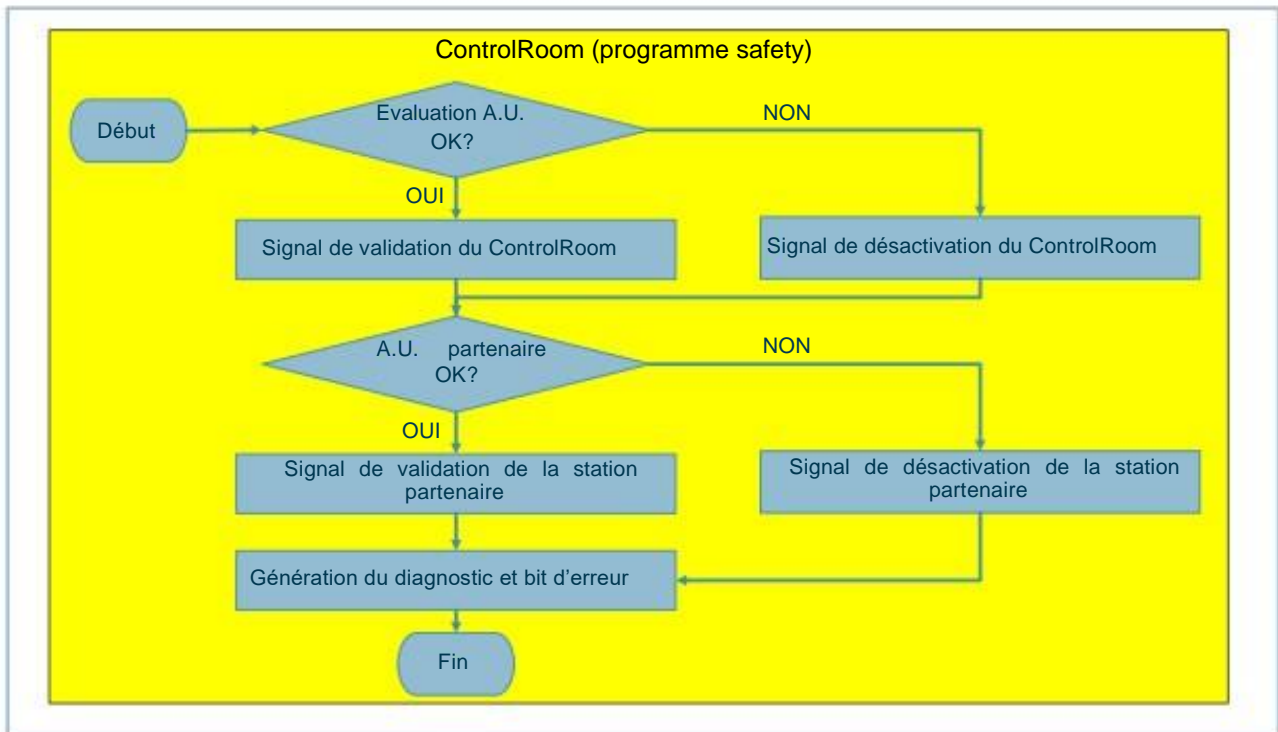
D:\.....

Suivez les étapes du chapitre 2.2 et observez la distribution des rôles lors des étapes de l'exercice

Remarque : Les étapes de l'exercice I-Device « plusieurs I-Device raccordés à un contrôleur » ne sont pas nécessaires. Les étapes de l'exercice pour IO-Contrôleur 10 à 13 ne sont pas nécessaire à votre application.

(Suite de l'exercice sur la page suivante)

7.9.1. Exercice 2 : Configurer la CPU



3. Lorsque vous avez réalisé la programmation comme dans l'exemple au chapitre 2.2, poursuivez avec la programmation au chapitre 2.3 « Communication IO-Controller-I-Device ».

Remarque : Il ne sera pas nécessaire de reprendre toutes les étapes si l'exercice 1 a été traité.

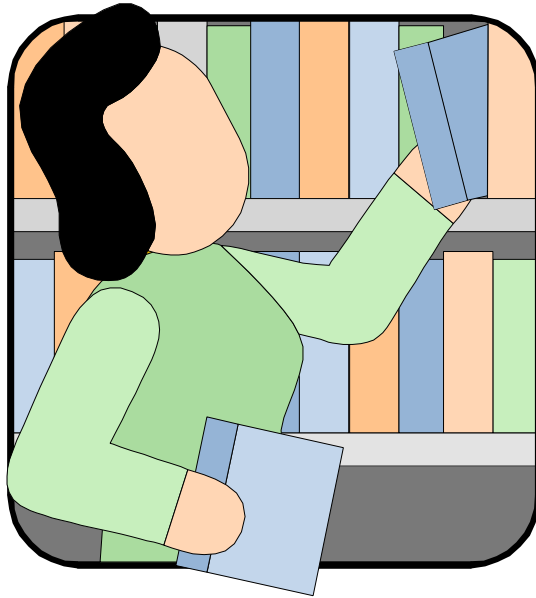
4. Intégrer la désactivation de la station partenaire au niveau de votre programme de sécurité (voir exercice 1 étape 12&13).
5. Chargez l'ensemble des blocs dans la CPU.
6. Sauvegardez votre projet et testez la fonction.

Résultat :

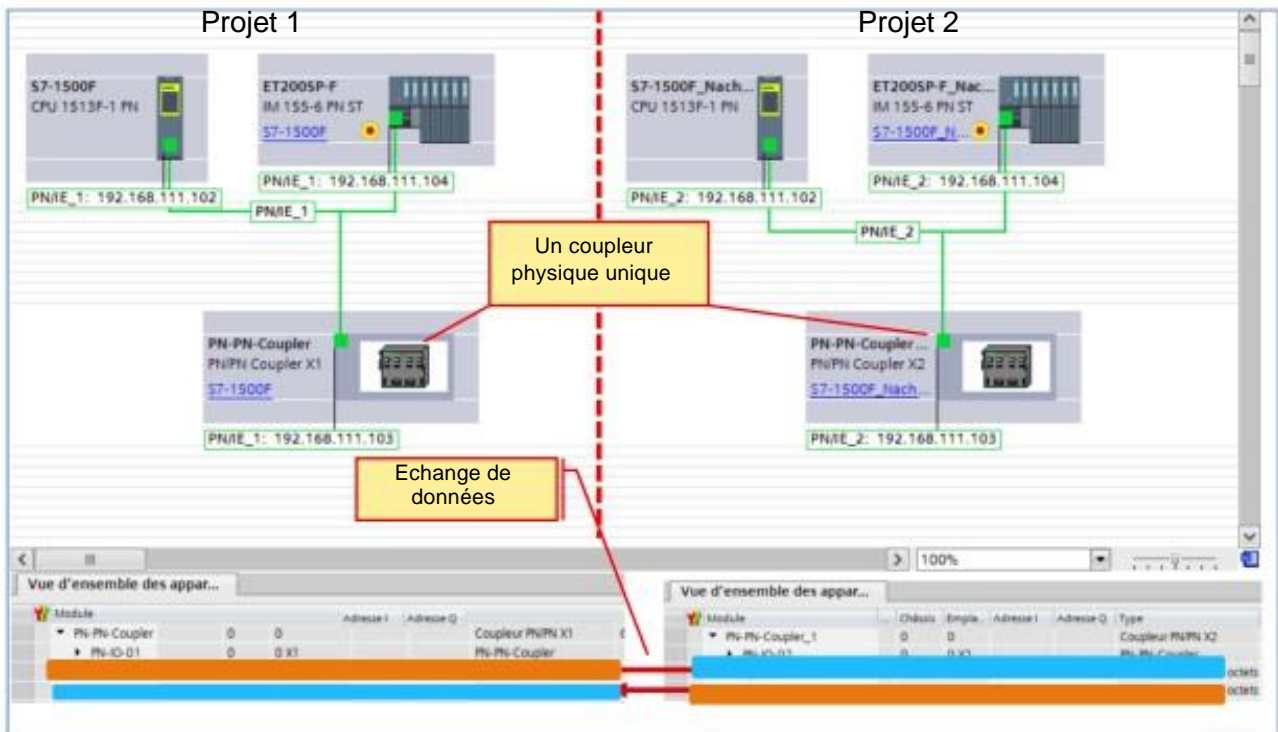
Les deux stations doivent maintenant pouvoir désactiver et amener l'installation du groupe partenaire dans un état sûr à l'aide de l'arrêt d'urgence du poste de commande (E2).

Remarque : Lors de la désactivation par la station partenaire il faut d'abord acquitter la station partenaire puis la propre station.

7.10. Informations



7.10.1. Programmation coupleur PN avec firmware v3.0 ou inférieur



Remarque

Dans l'éditeur « Appareils et réseaux », désactivez le paramètre d'affichage de validité des données DIA dans les propriétés du coupleur PN/PN. Il s'agit de la configuration par défaut. Si ce paramètre n'est pas désactivé, aucun transfert de données sécurisé ne peut être assuré entre des contrôleurs IO.

Création de zones de transfert

Pour chaque connexion de communication sécurisée entre deux CPU de sécurité, vous devez configurer une zone de transfert destinée aux données de sortie et une zone de transfert destinée aux données d'entrée pour le coupleur PN/PN dans l'éditeur « Appareils et réseaux ».

Règles de configuration pour les zones de transfert

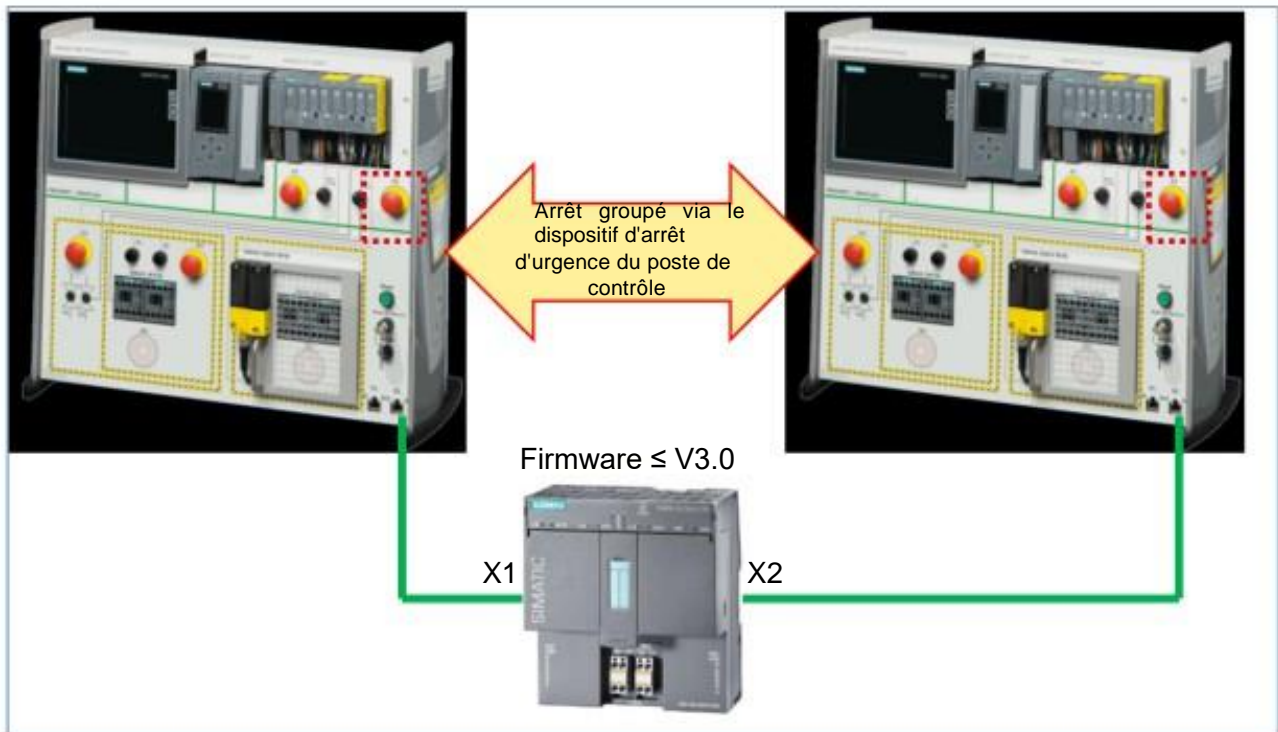
Données à émettre :

La zone de transfert destinée aux données de sortie doit pouvoir contenir 12 octets (données cohérentes). La zone de transfert destinée aux données d'entrée doit pouvoir contenir 6 octets (données cohérentes).

Données reçues :

La zone de transfert destinée aux données d'entrée doit pouvoir contenir 12 octets (données cohérentes). La zone de transfert destinée aux données de sortie doit pouvoir contenir 6 octets (données cohérentes).

7.10.2. Exercice 1 : Arrêt d'urgence global via coupleur PN avec firmware V3.0 ou inférieur



Enoncé

Actuellement chaque station travaille séparément sans liaison aux autres stations. Il faut maintenant réaliser une communication sûre entre 2 stations. La communication doit être réalisée via un coupleur PN/PN. Il doit être maintenant possible de désactiver la station partenaire via un arrêt d'urgence et inversement.

Préparation

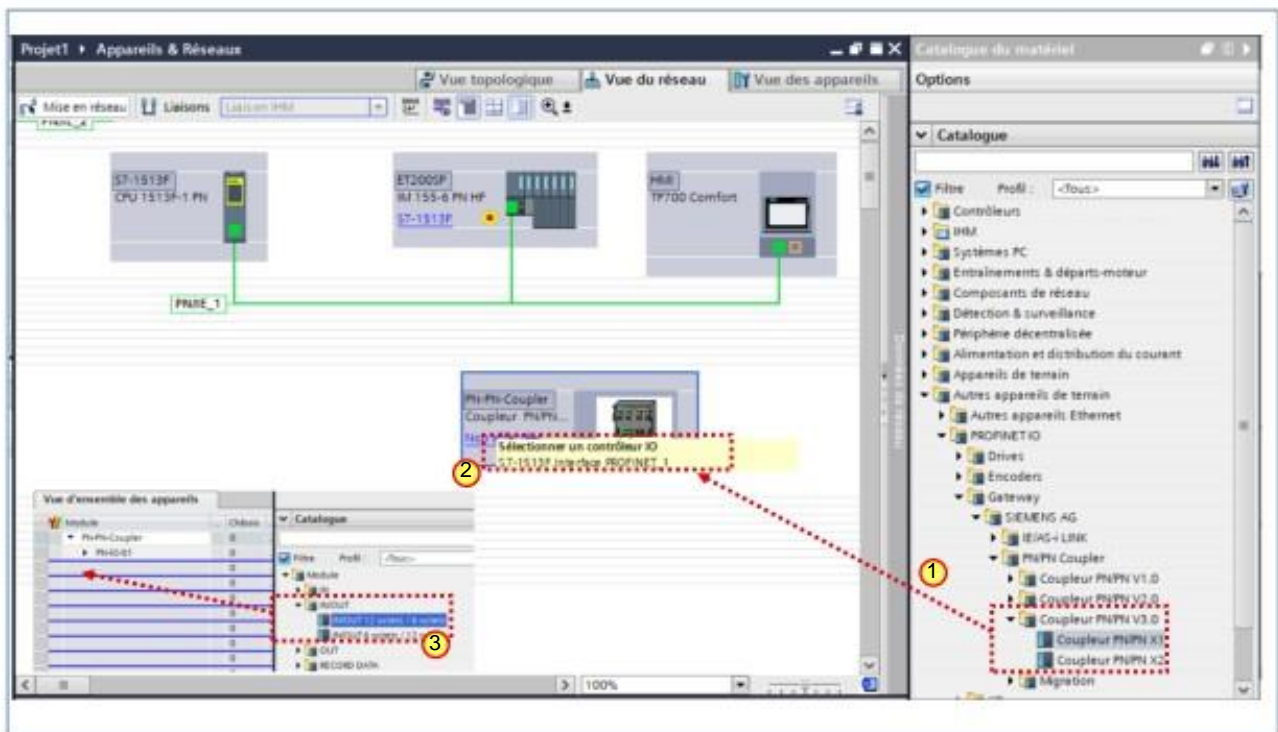
1. Intégrez une liaison PROFINET avec le coupleur PN-PN

Remarque

Synchronisez-vous avec le groupe partenaire au sujet des coupleur et des interface (X1,X2)

Suite page suivante

7.10.2.1. Exercice 1 : Configurer le coupleur PN-PN et les zones de transfert

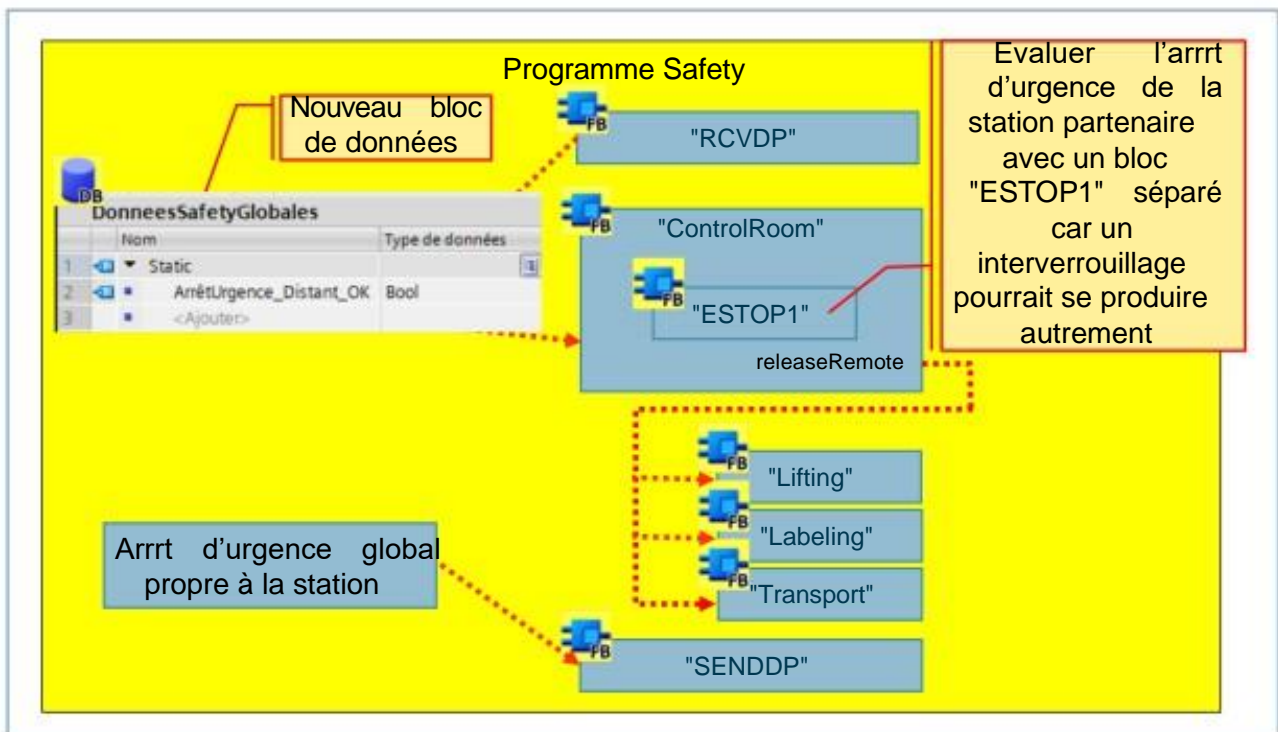


Procédure

1. Copiez par glisser-déposer la version correcte de l'interface et de votre coupleur DP/DP dans la vue du réseau
2. Insérez le coupleur dans le réseau de la CPU, adaptez le nom de l'appareil et son adresse IP (voir indications du schéma fourni).
3. Configurez le module de d'émission (IN/OUT 6Byte/12Byte) et le module de réception (IN/OUT 12Byte/6Byte)
Attention : synchronisez-vous avec le partenaire pour configurer l'emplacement des modules d'émission et de réception!
4. Affectez un nom en ligne au coupleur PN-PN.
5. Sauvegardez et chargez votre projet
6. L'ensemble de la station ne doit pas présenter d'erreur dès la fin du chargement de la station partenaire. Sinon vérifiez encore une fois le paramétrage et la liaison du coupleur PN-PN (des 2 groupes)

Suite prochaine page

7.10.2.2. Exercice 1 : paramétrer RCVDP et SENDDP



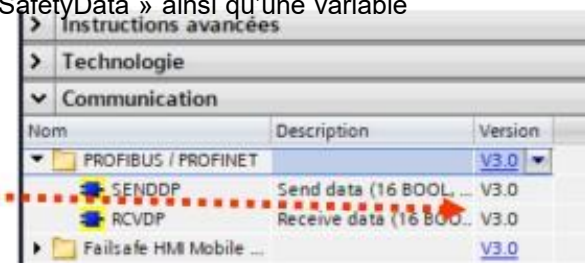
1. Créez un bloc de données global de sécurité « GlobalSafetyData » ainsi qu'une variable (Bool) "remoteEstopOk".
2. Appelez le bloc d'émission « SENDDP » et le bloc de réception « RCVDP » au bon endroit de votre programme de sécurité.

Remarque : Utilisez la version la plus récente des blocs!

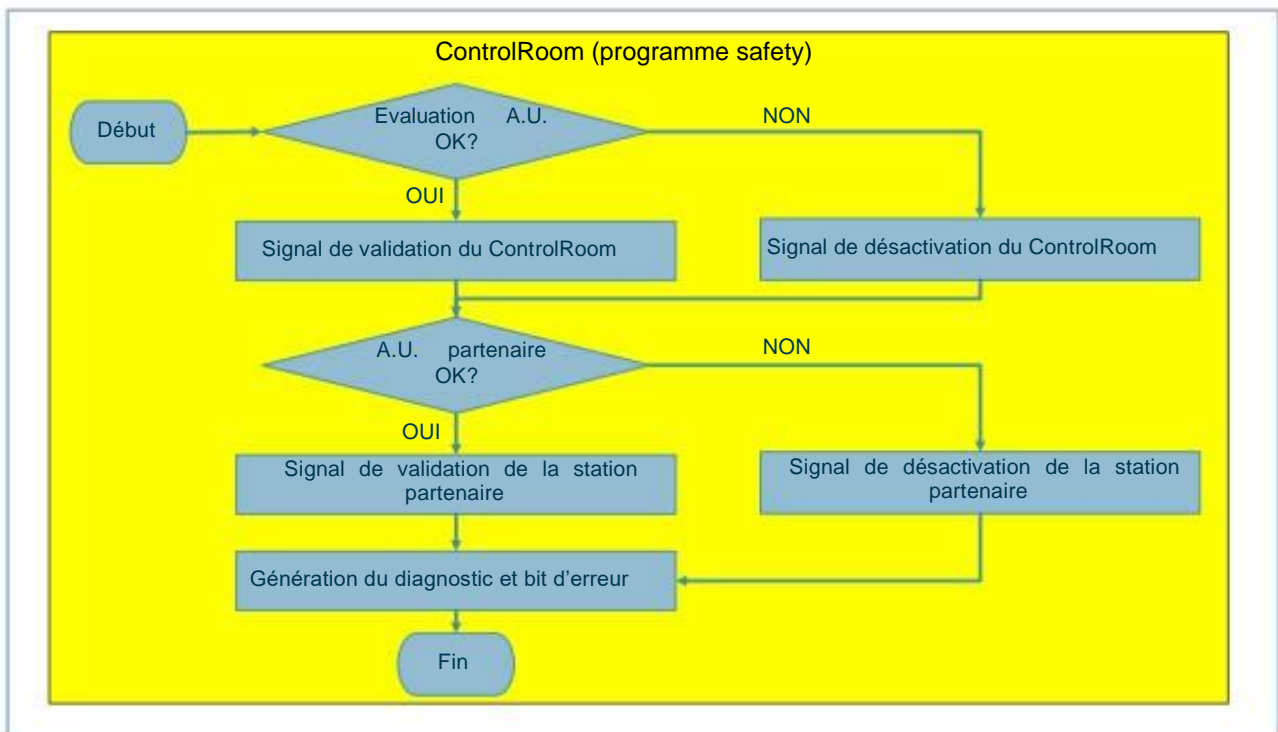
3. Transférez la libération globale de l'arrt d'urgence (E2) via le bloc d'émission « SENDDP » à la station partenaire.
4. Sauvegardez la libération de l'arrt d'urgence de la station partenaire dans la station partenaire "GlobalSafetyData".remoteEstopOk.
5. Paramétrez les autres interfaces nécessaires du bloc de données d'émission et de réception en fonction de la configuration de votre coupleur.

Remarque : il faut se synchroniser avec le groupe partenaire

Suite page suivante



7.10.2.3. Exercice 1 (suite) : Organigramme



1. Le signal d'acquiescement global de la station partenaire (« GlobalSafetyData ».remoteEstopOk) doit être considéré et exploité comme un nouvel arrrt d'urgence global indépendant. Évaluez le nouvel arrrt d'urgence dans le bloc « ControlRoom » par un nouvel appel de « ESTOP1 ».

Remarque : Si l'évaluation est déjà intégrée dans le module « ESTOP1 », alors il y aura un interverrouillage.

2. Adaptez la nouvelle désactivation globale à tous les éléments de l'installation. La fonctionnalité est identique à l'arrrt d'urgence global déjà en place.
3. Chargez l'ensemble des blocs dans la CPU.
4. Sauvegardez votre projet et testez la fonction.

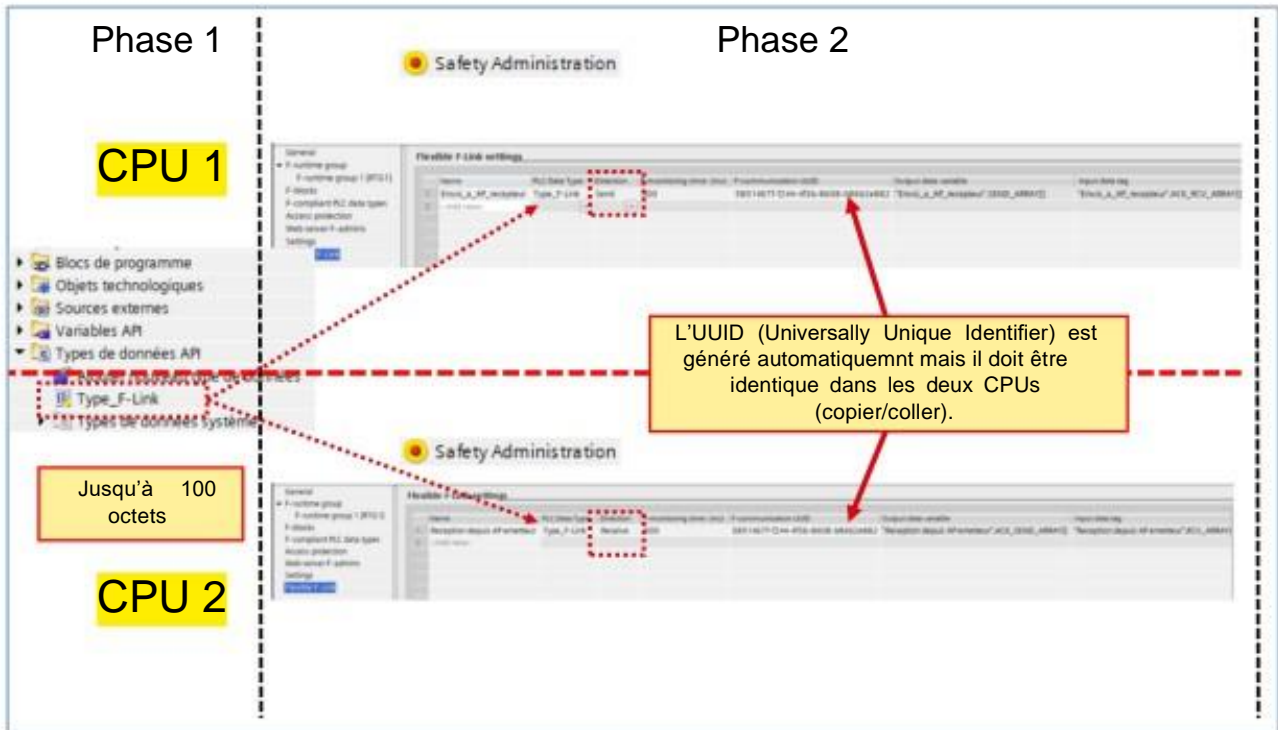
Résultat :

Les deux stations doivent maintenant pouvoir désactiver et amener l'installation du groupe partenaire dans un état sûr à l'aide de l'arrrt d'urgence du poste de commande (E2).

Remarque : Lors de la désactivation par la station partenaire il faut d'abord acquiescer la station partenaire puis la propre station.

7.10.3. Informations complémentaires F-Link

7.10.3.1. Paramétrage



Informations au sujet des communication F en place

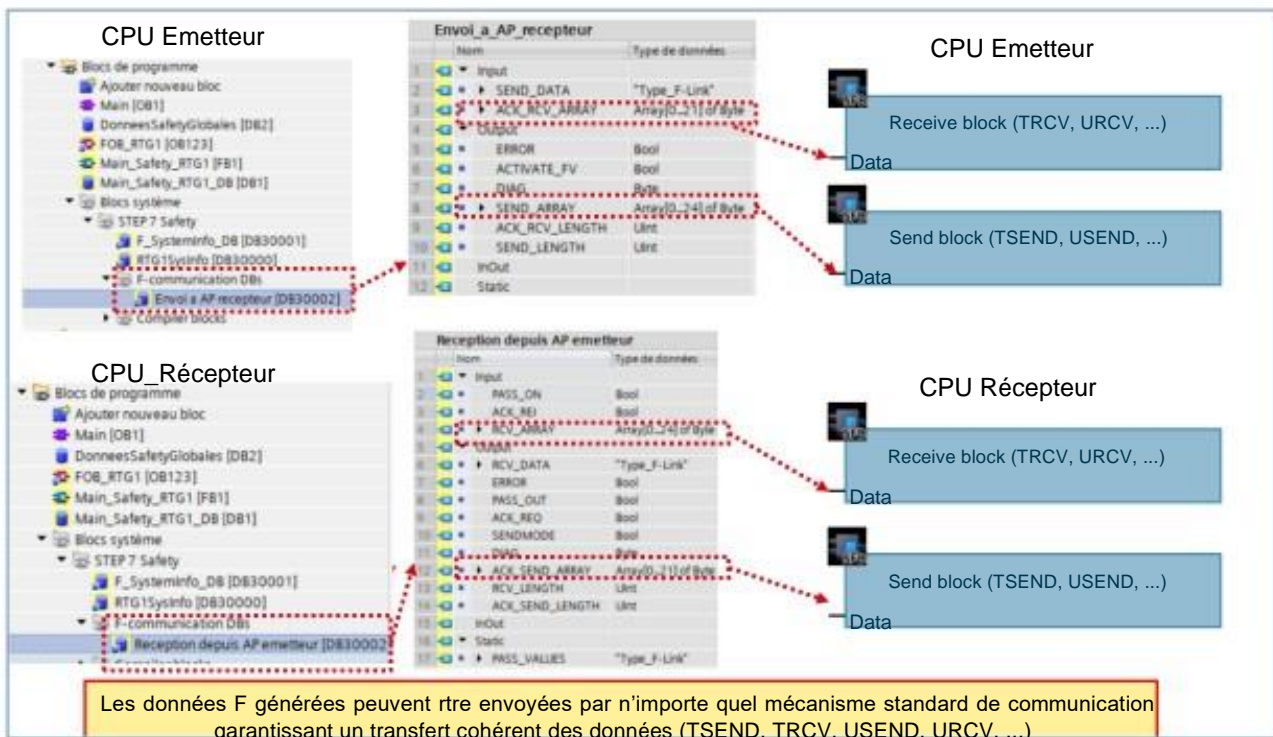
Sous « Flexible F-Link » vous obtenez des informations tabellaires au sujet des communications F paramétrées :

- Nom univoque du nom de la communication F pour la CPU
- Type de donnée API conforme (UDT) pour les données d'émission et de réception
- Direction de la communication F : émission/réception
- Temps de surveillance F de la communication F
- UUID de la communication F
- Les variables pour les données d'émission
- Les variables pour les données de réception

Attention

Lors de la création d'une nouvelle communication avec Flexible F-Link au niveau de l'éditeur d'administration, le système fournit un UUID pour la communication F univoque. La copie des communications de l'éditeur « Safety Administration » au sein du tableau de paramétrage ou la copie dans une autre CPU F ne régénère pas les UUID des communications F et elle ne reste donc pas univoque. Si la copie est utilisée pour paramétrer une nouvelle relation de communication il faudra assurer l'univocité. Sélectionnez pour cela les UUID concernés puis générez les une nouvelle fois via le menu contextuel « Générer UUID ». L'univocité doit être contrôlée lors de la réception du programme avec les documents de sécurité imprimés.

7.10.3.2. F-DB de communication



Transport de données de sécurité par des blocs de communication standard

Pour l'acheminement des tableaux codés de sécurité il faut intégrer au niveau du programme standard des blocs de communication qui assurent l'émission et la réception (Acquittement). Pour le traitement temporel correct des valeurs de processus vous disposez des OB F de pré et post traitement. Vérifiez lors de l'utilisation des blocs de communication standard que les tableaux F soient cohérents au moment de l'évaluation et que le temps de surveillance F soit tenu.

Utilisez les instructions standard pour la transmission des données cohérentes de

SEND_ARRAY :

- TSEND_C
- TSEND
- USEND

Utilisez les instructions standards pour la réception cohérente de ACK_RCV_ARRAY

- TRCV_C
- TRCV
- URCV

Table des matières

8.	Temps de réaction du système de sécurité	8-2
8.1.	Temps de réaction du système de sécurité : présentation synoptique.....	8-3
8.1.1.	Temps de réaction en cas d'absence d'erreur.....	8-4
8.2.	Table de calcul S7Safety_RTT	8-5
8.2.1.	Temps d'exécution maxi. du groupe d'exécution de la séquence du programme de sécurité (1).....	8-6
8.2.2.	Temps d'exécution maximum du groupe d'exécution de la séquence du programme de sécurité (2)	8-7
8.2.3.	Temps de surveillance minimum du programme de sécurité	8-8
8.2.4.	Temps de réaction maxi.....	8-9
8.2.5.	Temps de réaction type (1)	8-10
8.2.6.	Temps de réaction type (2)	8-11
8.2.7.	Temps de réaction type (3)	8-12
8.2.8.	Temps de réaction type (4)	8-13
8.2.9.	Temps de réaction type (5)	8-14
8.2.10.	Temps de réaction type (6)	8-15
8.2.11.	Temps de réaction type / Résultat	8-16
8.3.	Corrélation Temps de réaction / Distance minimale (norme ISO 13855).....	8-17

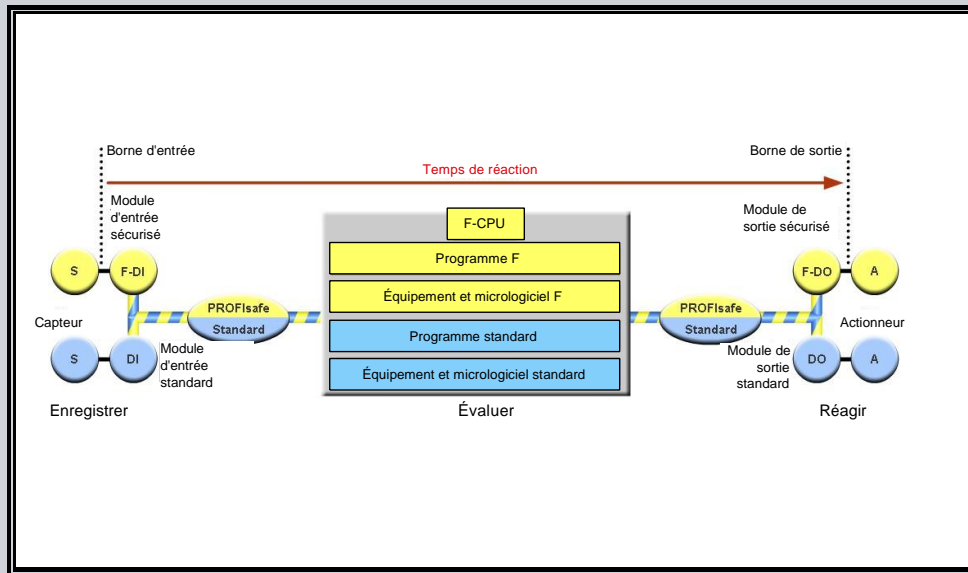
8. Temps de réaction du système de sécurité

À l'issue de la formation, le participant au stage

- ... connaîtra les différentes composantes permettant de déterminer le temps de réaction total
- ... pourra expliquer en quoi le temps de réponse d'une commande constitue une donnée critique en matière de sécurité des machines
- ... saura utiliser le tableau S7Safety_RTT



Temps de réaction du système de sécurité : aperçu

SITRAIN
TIA-SAFETY / Temps de réaction

Page 3

Siemens AG © 2014

Temps de réaction

Le temps de réaction, aussi appelé temps de réponse, est le temps qui s'écoule entre la détection d'un signal d'entrée et l'émission du signal de sortie par le module de sortie qui est combiné à cette entrée. Les distances de sécurité requises entre les points dangereux dans une installation dépendent principalement de la vitesse d'approche et du temps d'inertie de la machine. Pour les applications critiques en temps, il convient d'estimer le temps de réaction de l'automate de sécurité pour optimiser les distances de sécurité. Il est à noter que plus les distances de sécurité sont courtes, plus l'espace de travail est réduit, plus les coûts diminuent.

Marge de fluctuation

Le temps de réaction effectif se situe entre le temps de réaction minimum et le temps de réaction maximum. Pour configurer votre installation, vous devez toujours calculer le temps de réponse sur la base du temps de réaction maximum.

Temps de réaction maximum

Le temps de réaction maximum du système de sécurité est le temps le plus défavorable (worst case) pouvant s'écouler entre l'acquisition d'un signal de sécurité par le module d'entrée de sécurité et l'émission d'un signal par le module de sortie de sécurité.

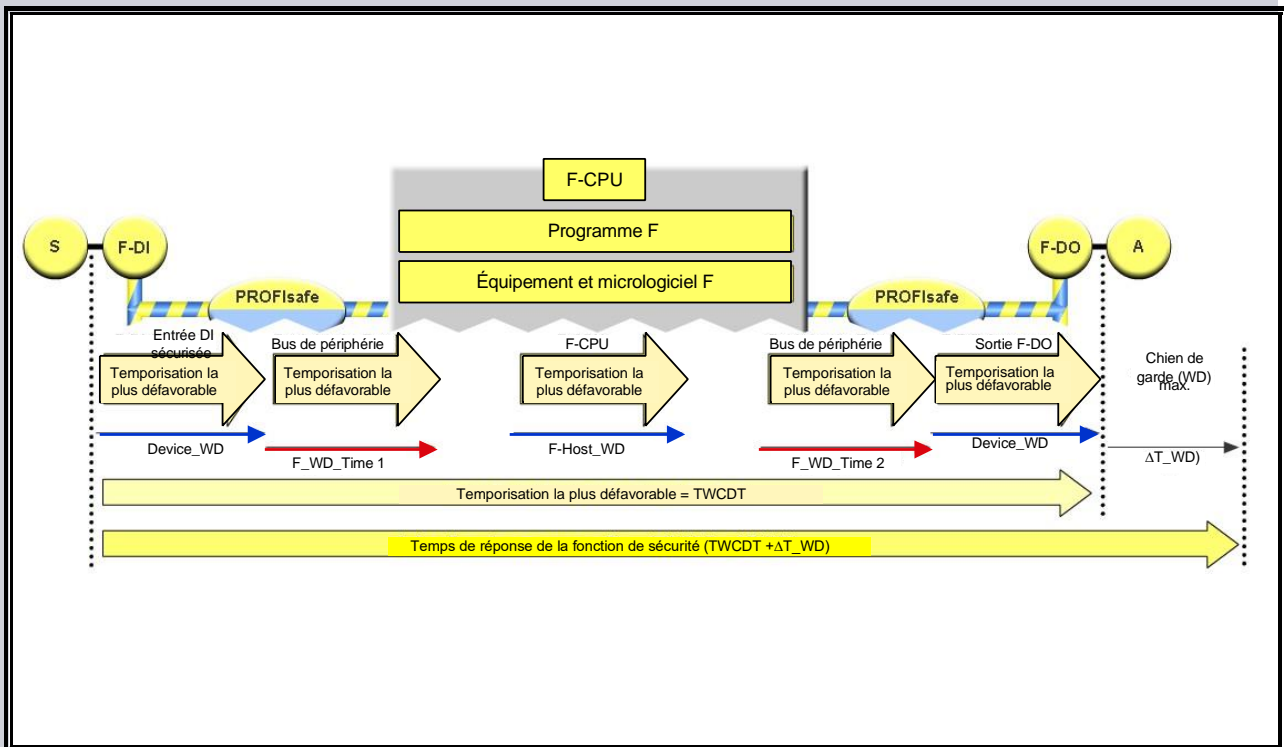
Programme standard

La CPU de sécurité exécute le programme standard et le programme de sécurité de manière indépendante. Le temps de cycle maximum possible (OB1) et le temps de réaction du programme standard est prolongé par l'exécution du programme de sécurité. Le temps de réaction dépend donc de l'ampleur du programme de sécurité et de la fréquence à laquelle la CPU l'exécute.

Programme de sécurité

Le temps de réaction du programme de sécurité est en revanche indépendant de la taille ou du temps d'exécution du programme standard. Le temps de réaction lors de l'exécution de la séquence de programme dédiée aux applications de sécurité est donc indépendant du temps d'exécution du programme standard.

Temps de réaction sans erreur



Temps de réponse des fonctions de sécurité (Safety Function Response Time)

Le temps « TWCDT + ΔT » correspond au temps de réaction total en cas d'absence d'erreur. Le temps « ΔT » tient compte des temporisations dans l'émission du signal aux points de transfert, le signal pouvant être acheminé seulement au cycle suivant, le cas échéant (scénario le plus défavorable).


Le temps maximum de réaction en cas d'absence d'erreur comprend...

- le temps d'acquittement maxi. du module de périphérie de sécurité (Device_WD)
- le temps d'exécution du programme de sécurité (F-Host_WD)
(composé de l'intervalle d'appel et du temps d'exécution du groupe d'exécution de la séquence de programme)
- du temps de rotation maxi. du système maître PROFIBUS-DP ou du temps d'actualisation maxi. sur les réseaux PROFINET IO (F_WD_Time 1/2).

8.2. Table de calcul S7Safety_RTT

Afin de vous aider à déterminer le temps de réaction total, vous pouvez consulter le fichier Excel disponible à l'adresse <http://support.industry.siemens.com/cs/document/93839056/simatic-step7-reaktionszeit-tabelle-safety-reaction-time-table-simatic-s7-1500f-s7-1200f?dti=0&lc=en-WW>

Ce tableau permet de déterminer en valeur approchée le temps d'exécution maxi. des groupes d'exécution du programme de sécurité, le temps de surveillance spécifique au programme de sécurité et le temps de réponse maxi. de votre système de sécurité.



Il convient toutefois de mesurer les valeurs effectives correspondant à votre installation, en tenant compte des actionneurs, des capteurs et des conditions d'exploitation sur le terrain. Le tableau S7Safety_RTTplus*.xls n'engage en rien son auteur sur le plan juridique. – ce titre, ce tableau ne saurait se substituer à une véritable recette technique effectuée sur site par un personnel qualifié, avec une documentation précise.

S7Safety_RTT

SIEMENS met à disposition gratuitement le tableau Excel « S7Safety_RTT » qui permet de calculer le temps maximum de réaction en cas d'absence d'erreur ainsi que les temps de surveillance du programme de sécurité lors de la configuration et de la programmation du projet.

8.2.1. Temps d'exécution maxi. du groupe d'exécution de la séquence du programme de sécurité (1)

Généralités			
FBD -et- LAD -[I]-, [NOT]- (Inverser RLO)		0,3 us	0,15 us
Opération sur bit			
FBD : &, >=1, X; LAD : montage en série, montage en parallèle par opérande	70	7,9 us	3,4 us
=	10	1,2 us	0,4 us
R, S		10 us	4,4 us
SR, RS	50	13 us	5,4 us
P, TRIG, N TRIG	50	14 us	5,9 us
Fonctions de sécurité			
ESTOP1	4	415 us	164 us
TWO_H_EN	1	397 us	157 us
MUT_P		1483 us	596 us
EV1to2DI		418 us	165 us
FDBACK	2	463 us	183 us
SFDOOR	1	298 us	118 us
ACK_GL	1	22 us	8,8 us
Temporisations, temporisations IEC			
TP		335 us	132 us
TON		374 us	148 us
TOF		374 us	148 us
Compteurs, compteurs IEC			
CTU		213 us	84 us
CTD		220 us	87 us
CTUD		429 us	169 us
Comparateur			
CMP ==, <=		19 us	8,1 us
CMP >, <, >=, <=		14,4 us	6,1 us
Fonctions mathématiques			
ADD		8,1 us	3,5 us
SUB		11 us	4,5 us
MUL		16 us	6,5 us
DIV		57 us	22 us
NEG		7,4 us	3,1 us
Déplaceur			
MOVE	2	1,5 us	0,6 us
Convertisseur			
CONVERT INT->DINT		6,5 us	2,5 us
BO_W		74 us	29 us
W_BO		63 us	25 us
SCALE		329 us	124 us

SIMATIC STEP7 Safety V13 Reaction Time Table SIMATIC S7-1500F

Le tableau d'estimation du temps de réaction S7Safety Reaction Time Table (S7Safety_RTTplus*.xls) permet d'estimer, sur le plan purement théorique, le temps d'exécution des séquences de programme de sécurité, le temps de surveillance et le temps de réponse de la CPU SIMATIC S7-1500F dès la phase de configuration du projet. Les temps d'exécution des blocs d'application de sécurité et des éléments de programme F-FBD (LOG) / F-LAD (CONT) ainsi que le temps d'exécution du groupe d'exécution de la séquence de programme de sécurité sont déterminés à partir du logiciel SIMATIC STEP7 Safety Advanced. S'agissant d'une estimation théorique, il convient de mesurer les valeurs effectives en situation réelle, en tenant compte des actionneurs, des capteurs et des conditions d'exploitation sur le terrain. Le fichier S7Safety_RTTplus*.xls n'engage pas son auteur sur le plan juridique. - ce titre, il ne saurait se substituer une recette technique sur site par un personnel qualifié et ne doit pas figurer dans la documentation de l'installation.

8.2.2. Temps d'exécution maximum du groupe d'exécution de la séquence du programme de sécurité (2)

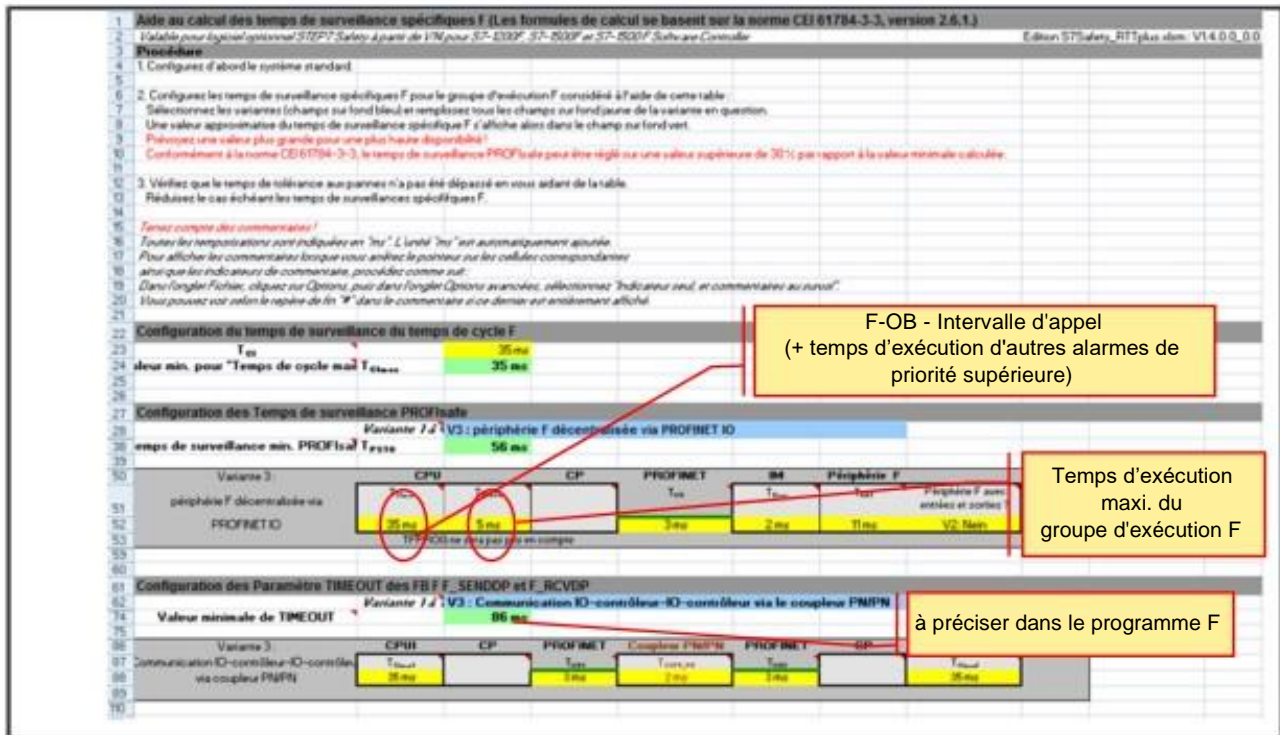
Commande du programme			
JMP, JMPN, RET		31 us	11,7 us
Opérations sur word			
AND, OR, XOR		9,5 us	4,0 us
Déplacer + tourner			
SHR		79 us	31 us
SHL		106 us	42 us
Commander			
ACK, OP	1	242 us	91 us
Communication			
PROFIBUS / PROFINET			
SENDOP	1	234 us	93 us
RCVOP	1	327 us	129 us
FB F/FC F de la bibliothèque globale ou instructions issues d'autres logiciels optionnels			
Somme des temps d'exécution	1	0 us	0 us
Appels de bloc			
CALL FB F / FC F	3	6,2 us	2,4 us
Paramètre d'entrée		1,4 us	0,5 us
Paramètre de sortie		0,8 us	0,3 us
Paramètre d'entrée/sortie		2,0 us	0,7 us
Données locales statiques		0,0 us	0,0 us
Conversion du type de données en cas de type de données différent			
Nombre de paramètres du type de données INT ou WORD qui sont connectés à un opérande avec un type de données différent (WORD au lieu de INT ou INT au lieu de WORD)		2,7 us	1,0 us
Temps d'exécution max. du groupe d'exécution F (TFPROG)		11 ms	5 ms

Temps d'exécution dans les conditions d'exploitation

Le temps maximum d'exécution du groupe d'exécution F (TFPROG) peut être rallongé notamment par la charge de communication (ex. communication S7, communication PROFINET E/S, communication PG/OP), par l'exécution des alarmes de priorité haute et par les fonctions de test et de mise en service.

Vous pouvez mesurer l'incidence de ces facteurs en vous référant à la documentation et à la configuration du système standard.

8.2.3. Temps de surveillance minimum du programme de sécurité



Temps de surveillance du programme de sécurité

Vous disposez de deux possibilités pour configurer le temps de surveillance de la communication sécurisée entre la CPU et le module de périphérie de sécurité :

- Dans l'éditeur permettant de paramétrer la CPU F (propriétés de la CPU) ou
- Lors du paramétrage du module de périphérie de sécurité, dans les propriétés du module de périphérie

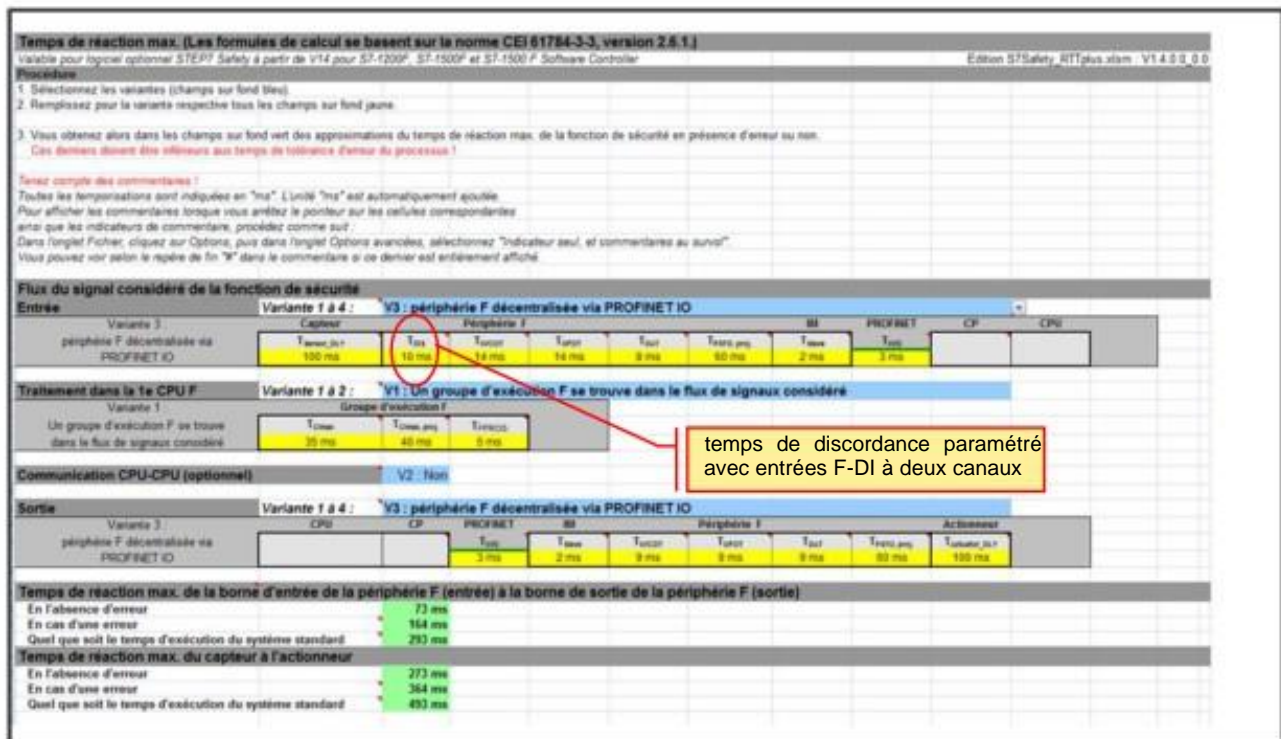
Temps de surveillance PROFIsafe TPSTO

La valeur du temps de surveillance PROFIsafe TPSTO doit être suffisamment importante pour ne pas déclencher la surveillance en cas d'absence d'erreur.

Paramètre de TIMEOUT pour les instructions SENDDP et RCVDP

La surveillance du temps s'effectue via les instructions SENDDP et RCVDP ou SENDS7 et RCVS7 du partenaire de communication. Le paramètre de TIMEOUT du temps de surveillance doit être identique pour les deux instructions. La valeur du TIMEOUT doit être suffisamment importante pour ne pas déclencher la surveillance en cas d'absence d'erreur.

8.2.4. Temps de réaction maxi.



Temps de réaction maximum

Le temps de réaction maximum du système de sécurité est le temps le plus défavorable (durée la plus longue possible) pouvant s'écouler entre l'acquisition d'un signal de sécurité par le module d'entrée de sécurité et l'émission d'un signal de sécurité par le module de sortie de sécurité.

Règle relative au temps de réaction maximum d'une fonction de sécurité

Le temps de réaction maximum d'une fonction de sécurité doit être inférieur au temps de tolérance aux défauts du processus.

Temps de réaction en l'absence d'erreur

Il s'agit du temps de réponse requis en situation réelle. Les mesures suivantes permettent d'optimiser les temps de réaction :

- Raccourcir l'intervalle d'appel du groupe d'exécution de la séquence du programme de sécurité
- Accélérer le transfert via le bus (par exemple : augmenter le débit du réseau PROFIBUS)
- Passivation au niveau des modules
- Optimiser en temps les modules F-DI (ETOR de sécurité) (par exemple : optimiser le temps de discordance, en tenant compte des impératifs de la fonction de sécurité)
- Utiliser une CPU plus rapide

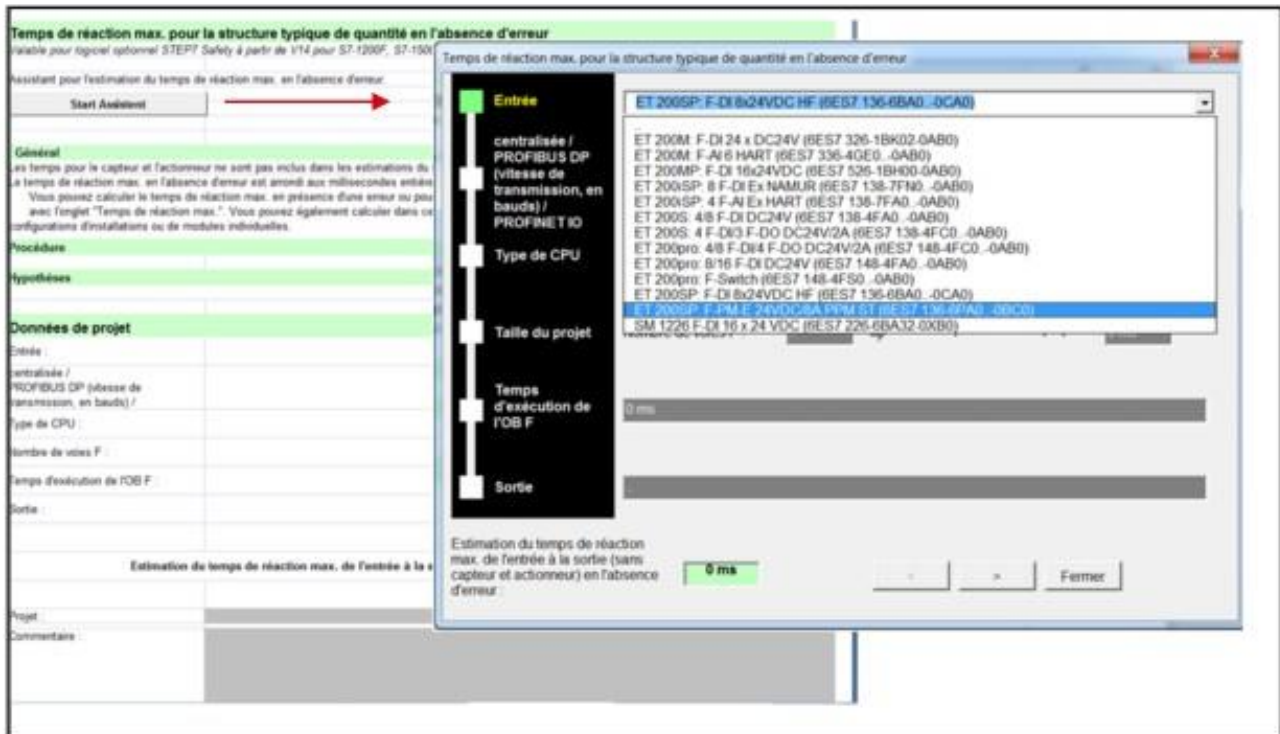
... en cas d'erreur

Uniquement en cas d'erreurs multiples, conformément à la norme CEI 61508.

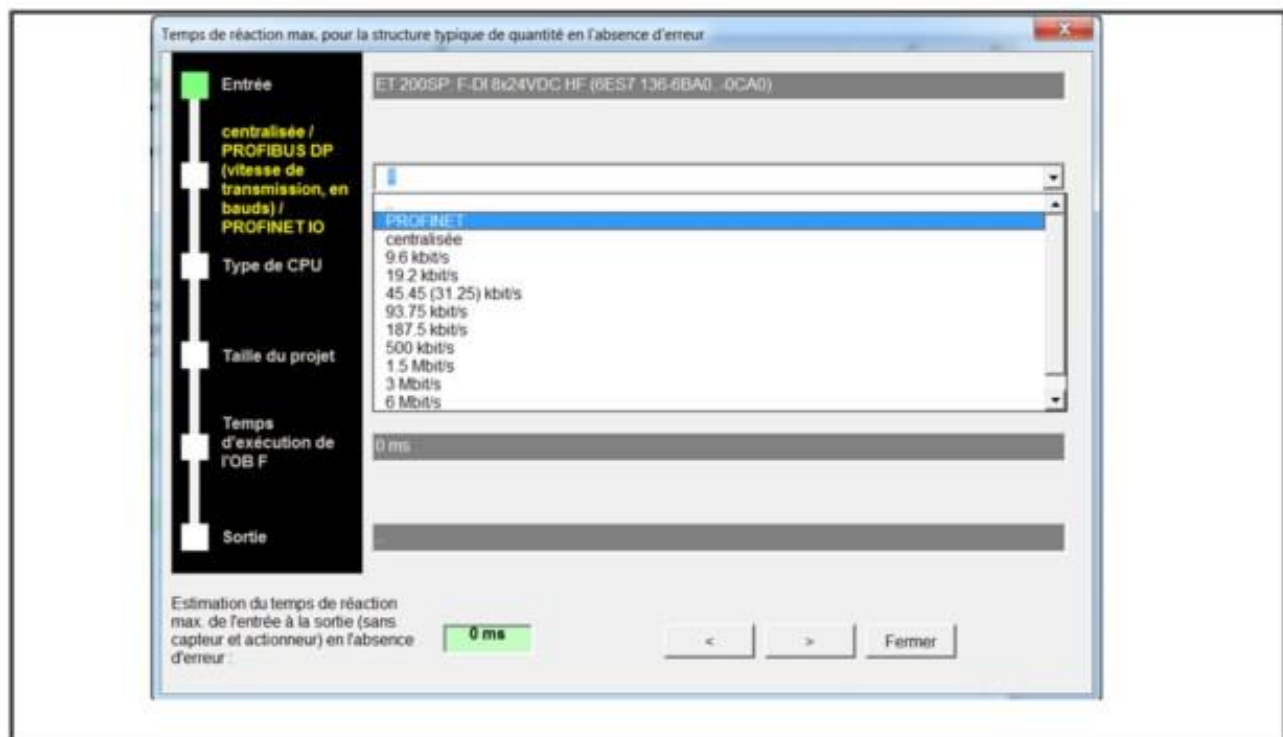
... quel que soit le temps d'exécution du système standard

Uniquement si le groupe d'exécution de la séquence du programme de sécurité a été appelé par des OB de priorité inférieure (par exemple OB1) et peut donc être interrompu par des OB de priorité supérieure (par exemple FOB).

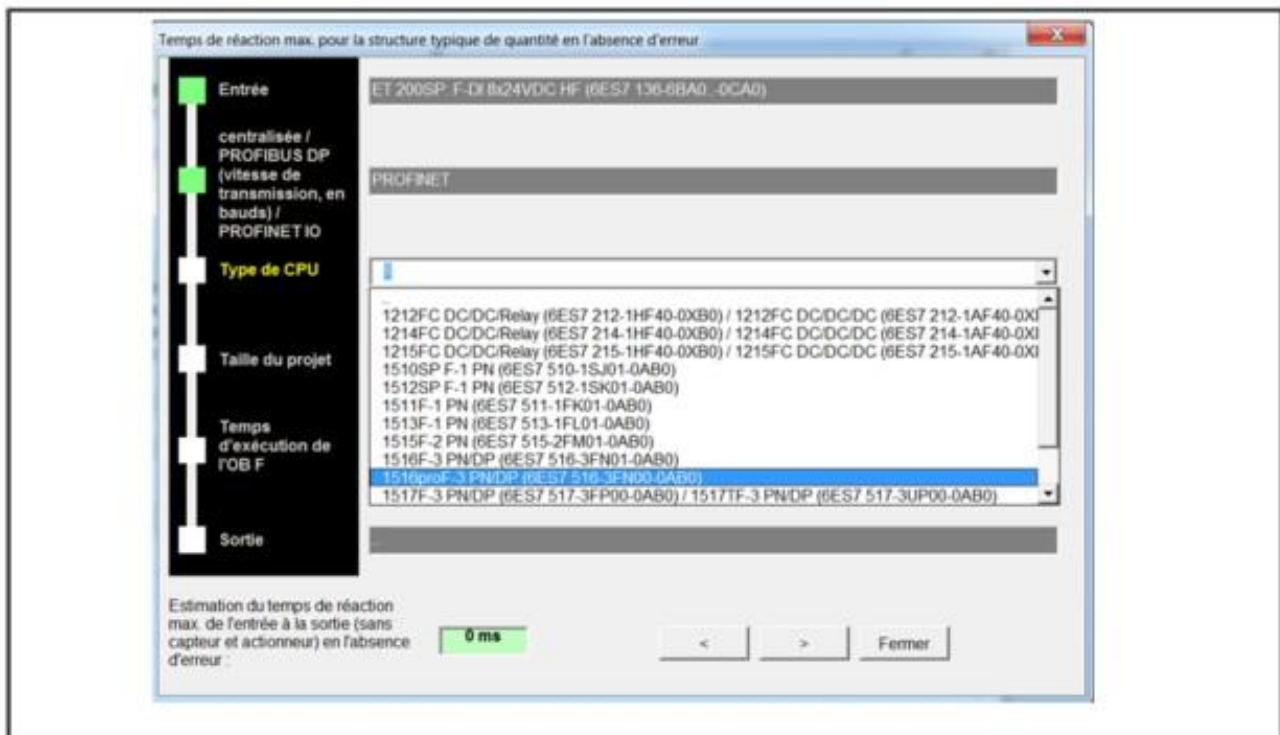
8.2.5. Temps de réaction type (1)



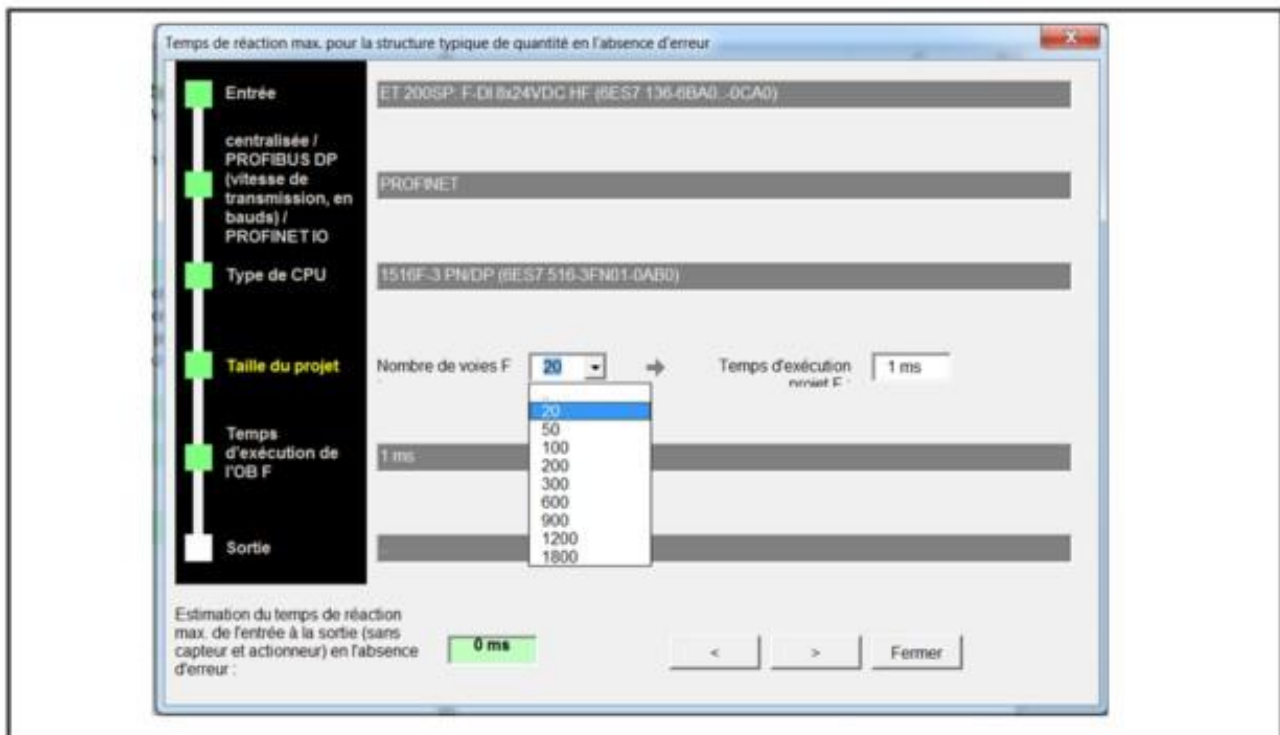
8.2.6. Temps de réaction type (2)



8.2.7. Temps de réaction type (3)



8.2.8. Temps de réaction type (4)



8.2.9. Temps de réaction type (5)

Temps de réaction max. pour la structure typique de quantité en l'absence d'erreur

Entrée
centralisée /
PROFIBUS DP
(vitesse de
transmission, en
bauds) /
PROFINET IO
Type de CPU
Taille du projet
Temps
d'exécution de
l'OB F
Sortie

ET 200SP F.DI 6x24VDC HF (6ES7 136-8BA0...0CA0)

PROFINET

1516F-3 PN DP (6ES7 516-3FN01-0AB0)

Nombre de voies F 20 ⇒ Temps d'exécution normal F 1 ms

100 ms

10
50
100
500
1000
2000

Estimation du temps de réaction
max. de l'entrée à la sortie (sans
capteur et actionneur) en l'absence
d'erreur :

0 ms

< > Fermer

8.2.10. Temps de réaction type (6)

Temps de réaction max. pour la structure typique de quantité en l'absence d'erreur

Entrée	ET 200SP F-DI 8x24VDC HF (6ES7 136-6BA0-0CA0)	
centralisée / PROFIBUS DP (vitesse de transmission, en bauds) / PROFINET IO	PROFINET	
Type de CPU	1516F-3 PN/DP (6ES7 516-3FN01-0AB0)	
Taille du projet	Nombre de voies F : 20 → Temps d'exécution nominal C :	1 ms
Temps d'exécution de l'OB F	100 ms	
Sortie	ET 200SP F-DQ 4x24VDC/2A PM HF (6ES7 136-6DB0-0CA0)	

Estimation du temps de réaction
max. de l'entrée à la sortie (sans
capteur et actionneur) en l'absence
d'erreur :

158 ms

< > Fermer

8.2.11. Temps de réaction type / Résultat

Assistant pour l'estimation du temps de réaction max. en l'absence d'erreur.

Assistant de démarrage

Général

Les temps pour le capteur et l'actionneur ne sont pas inclus dans les estimations du temps de réaction.
 Le temps de réaction max. en l'absence d'erreur est arrondi aux millisecondes entières et constitue l'estimation la plus pessimiste.
 Vous pouvez calculer le temps de réaction max. en présence d'une erreur ou pour des temps d'exécution quelconques du système standard avec l'onglet "Temps de réaction max.". Vous pouvez également calculer dans cet onglet les temps de réaction max. en l'absence d'erreur pour des configurations d'installations ou de modules individuelles.

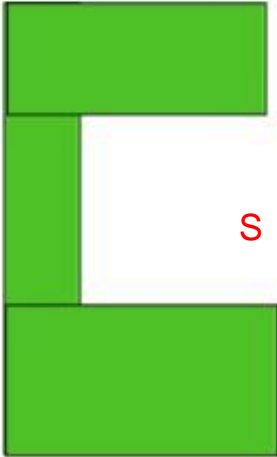
Procédure

Hypothèses

Données de projet

Entrée :	ET 200SP: F-DI 8x24VDC HF (6ES7 136-6BA0...-0CA0)
centralisée / PROFIBUS DP (vitesse de transmission, en bauds) /	PROFINET
Type de CPU :	1516F-3 PN/DP (6ES7 516-3FN01-0AB0)
Nombre de voies F :	20
Temps d'exécution de FOB F :	100 ms
Sortie :	ET 200SP: F-DQ 4x24VDC/2A PM HF (6ES7 136-6DB0...-0CA0)
Estimation du temps de réaction max. de l'entrée à la sortie (sans capteur et actionneur) en l'absence d'erreur :	
	158 ms

8.3. Corrélation Temps de réaction / Distance minimale (norme ISO 13855)



Formule générale de calcul :

$$S = K \times T + C \text{ en cas d'approche à angle droit}$$

S = Distance minimale en mm
K = Vitesse d'approche 2 mm/ms
T = $t_1 + t_2 + t_3$ en ms
 t_1 : temps de réponse des équipements de protection électrosensibles (ESPE)
 t_2 : temps de réponse de l'interface de sécurité
 t_3 : temps d'arrêt de la machine
C = $8 \times (d - 14)$ en mm (distance supplémentaire)
d = résolution de l'ESPE (plage de 14 à 40 mm)

Distance minimale et règles d'installation des équipements de protection

Les équipements de protection électrosensibles ne peuvent remplir leur fonction de sécurité que si une distance minimale est respectée. Le calcul de la distance minimale de sécurité dépend du type de protection mis en œuvre. La norme harmonisée ISO 13855 « Positionnement des moyens de protection par rapport à la vitesse d'approche des parties du corps » (anciennement EN 999) permet de déterminer les emplacements de montage et de choisir le mode de calcul approprié pour déterminer la distance minimale de sécurité en fonction du dispositif de protection mis en œuvre.

Les distances de sécurité entre les points dangereux dépendent principalement de la vitesse d'approche et du temps d'inertie de la machine.

Pour les applications critiques en temps, il convient d'estimer le temps de réaction de l'automate de sécurité (cf. la formule de calcul ci-dessus : t_2 = temps de réponse de l'interface de sécurité) pour optimiser les distances de sécurité.

Définition du temps de tolérance aux défauts de processus

Le temps de tolérance aux défauts issus du processus correspond à la durée pendant laquelle un processus peut être exploité en toute autonomie sans entraîner de risques pour l'intégrité physique du personnel ni de dommages pour l'environnement. Le temps de tolérance aux défauts de processus dépend du type de processus. Il doit être défini individuellement.

Table des matières

9.	Réception d'une installation.....	9-2
9.1.	Base juridique : Directive Machines.....	9-2
9.2.	Marche à suivre pour une machine sûre selon la directive Machines	9-3
9.3.	Qu'est-ce que la validation ?.....	9-4
9.4.	Insertion de la validation globale (essais de réception) dans le modèle de processus	9-5
9.5.	Vérification < > Validation	9-6
9.6.	Mesures de validation avant la validation globale du produit	9-7
9.7.	Validation de l'application globale.....	9-8
9.8.	Personnes autorisées et procès-verbal de réception	9-9
9.9.	Contenu d'un essai de réception complet.....	9-10
9.10.	Impression de sécurité	9-11
9.10.1.	Création d'une impression de sécurité	9-12
9.10.2.	Marche à suivre pour la création d'une impression de sécurité	9-13
9.10.3.	Exemple d'impression de sécurité	9-14
9.11.	Réception des modifications	9-15
9.12.	Exercice 1 : Réalisation d'un essai de réception	9-16
9.12.1.	Exercice 1 : Description de la documentation relative à l'essai	9-17
9.12.2.	Exercice 1 (suite) : Essais avant la mise en marche	9-18
9.12.3.	Exercice 1 (suite) : Essais en cours de service : Dispositif de levage	9-19
9.12.4.	Exercice 1 (suite) : Essais en cours de service : Etiqueteuse (1).....	9-20
9.12.5.	Exercice 1 (suite) : Essais en cours de service : Etiqueteuse (2).....	9-21
9.12.6.	Exercice 1 (suite) : Essais en cours de service : Robot Mode automatique (1)	9-22
9.12.7.	Exercice 1 (suite) : Essais en cours de service : Robot Mode automatique (2)	9-23
9.12.8.	Exercice 1 (suite) : Essais en cours de service : Robot Mode maintenance.....	9-24
9.12.9.	Exercice 1 (suite) : Essais en cours de service : Test d'injection de défauts	9-25
9.12.10.	Exercice 1 (suite) : Résultat	9-26
9.13.	Exercice 2 : « Mesure temps d'arrêt » Moteur 2 via Trace.....	9-27
9.13.1.	Exercice 2 (suite) : Créer une Trace	9-28
9.13.2.	Exercice 2 (suite) : Charger, démarrer et enregistrer une Trace	9-29

9. Réception d'une installation

9.1. Base juridique : Directive Machines

DIRECTIVE 2006/42/CE DU PARLEMENT EUROPEEN ET DU CONSEIL du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (refonte)

(19) Au vu de la nature des risques liés à l'utilisation des machines couvertes par la présente directive, il convient d'établir des procédures d'évaluation de la conformité aux exigences essentielles de santé et de sécurité. Ces procédures devraient être conçues eu égard à l'importance du danger inhérent à ces machines. Par conséquent, chaque catégorie de machines devrait être assortie d'une procédure adéquate qui soit conforme à la décision 93/465/CEE du Conseil du 22 juillet 1993 concernant les modules relatifs aux différentes phases des procédures d'évaluation de la conformité et les règles d'apposition et d'utilisation du marquage « CE » de conformité, destinés à être utilisés dans les directives d'harmonisation technique, et qui tiennent compte de la nature de la vérification requise pour ces machines.

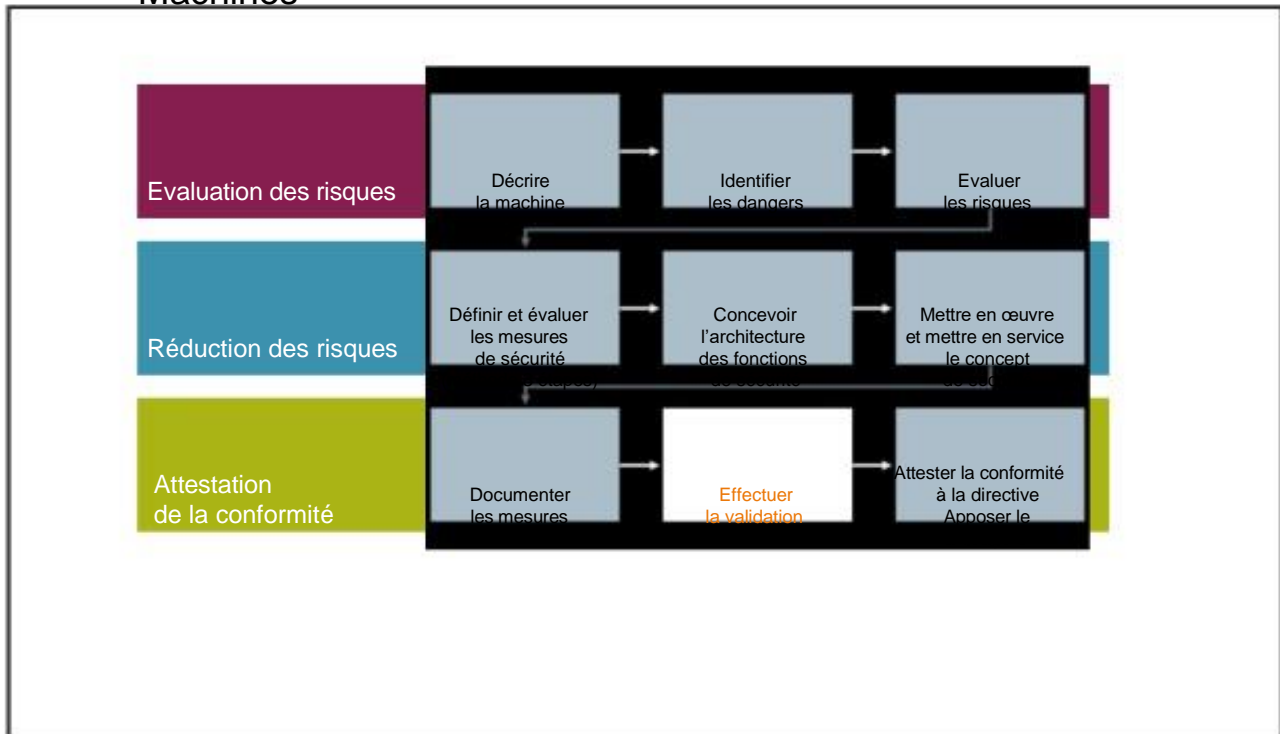


Réception d'une installation

Lors de la réception d'une installation, il convient de respecter toutes les normes pertinentes spécifiques au domaine d'application. Ceci vaut également pour les installations non soumises à une obligation de réception. Lors de la réception, vous devez respecter les obligations figurant dans le rapport de certification. La réception d'un système F est généralement effectuée par un expert indépendant.

9.2. Marche à suivre pour une machine sûre selon la directive

Machines



La validation est l'une des phases du modèle de processus à suivre pour le développement d'une machine sûre. Elle s'applique à l'ensemble de la machine. Cette phase englobe la validation du système de sécurité.

9.3. Qu'est-ce que la validation ?

Selon les normes EN ISO 13849-2 (version 2012) et EN 62061, la validation est la vérification d'un système de sécurité sous les aspects suivants :

- Les exigences de la **spécification de sécurité (SRS)** sont-elles correctement et efficacement mises en œuvre ?
- Les **fonctions de sécurité de la machine** sont-elles correctement mises en œuvre ?
- La mise en œuvre répond-elle aux **caractéristiques** et à la **qualité requises en matière de techniques de sécurité** ?

Objectif de la validation

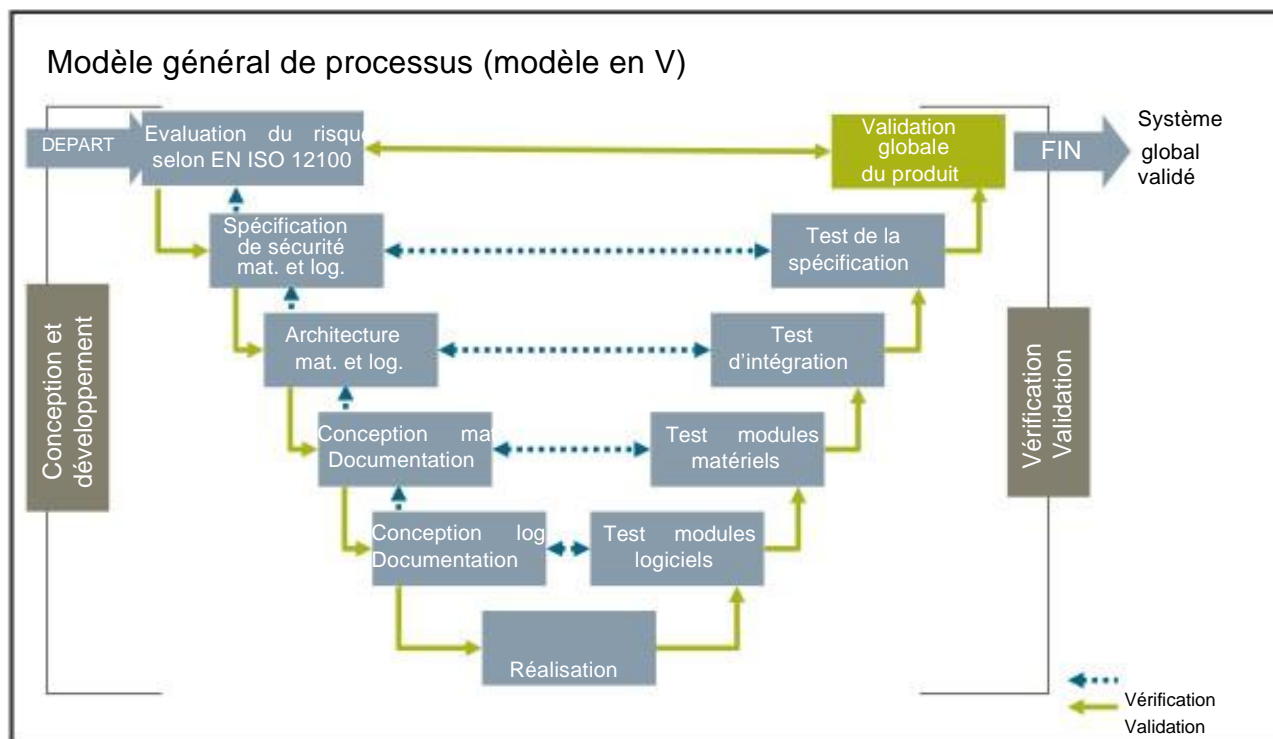
L'objectif de la validation est d'attester que les fonctions de sécurité mises en œuvre apportent la contribution nécessaire à la réduction des risques afin que la machine soit et reste sûre.

La réduction des risques est obtenue grâce aux fonctions de sécurité et à d'autres mesures (constructives, techniques, organisationnelles).

SRS est l'abréviation de Safety Requirements Specification (spécification des exigences de sécurité).

Les normes CEI 51508-2 (Annexe B) et CEI 61508-3 (Annexe A) décrivent en outre des procédures pour éviter les défaillances systématiques. Leur respect accroît la qualité des fonctions de sécurité et contribue au succès de la validation.

9.4. Insertion de la validation globale (essais de réception) dans le modèle de processus



Le modèle en V représenté est le modèle générique pour le développement et la validation d'un système de sécurité.

9.5. Vérification < > Validation

Définitions de la vérification et de la validation selon EN 62061 :

Vérification



Validation

Confirmation par examen (par ex.

essais, analyses) que le système relatif à la sécurité et les parties du système relatif à la sécurité satisfont aux exigences des spécifications correspondantes.

Activités en pointillés bleus dans le modèle en V (vérification de l'exécution correcte des différentes phases)

9-6



Vérification :

Démontrer la vérité

Validation :

Vérifier l'efficacité

Confirmation par examen (par ex.
essais, analyses) que le système
relatif à la sécurité satisfait aux
exigences de sécurité
fonctionnelle pour une application spécifique.

Activités en lignes

vertes continues dans le modèle en V (vérification de l'adéquation
de l'application)


9.6. Mesures de validation avant la validation globale du produit




Que devez-vous valider ?

1. Spécification des fonctions de sécurité
-> par ex. revue de la spécification
2. Concept de réalisation, architecture et fiabilité
-> par ex. SET (Safety Evaluation Tool)
3. Mise en œuvre matérielle
-> Analyse du schéma et du câblage/configuration matérielle
4. Mise en œuvre logicielle
-> Vérification (revue) logiciel, documentation et diagrammes de flux
5. Application globale (essai de réception)

9.7. Validation de l'application globale

 Que devez-vous valider ?

1. Mise en œuvre et fonctionnement correct des fonctions de sécurité
2. Robustesse de la mise en œuvre des fonctions de sécurité en cas d'apparition de défauts

 Objectif de la validation :

L'objectif de la validation est d'attester que les fonctions de sécurité ont été mises en œuvre conformément aux exigences, que le logiciel (d'application) concourt à l'exécution correcte des fonctions de sécurité et que les mesures de prévention des défauts sont efficaces.

 Comment devez-vous procéder ?

Effectuez un contrôle de fonctionnement des fonctions de sécurité à l'aide d'un « test en boîte noire ». Réalisez des simulations de défauts (tests d'injection de défauts) sur la base des résultats des analyses effectuées.

Avant de procéder aux contrôles de fonctionnement, vous devez vérifier que la configuration correcte est bien activée dans le système de sécurité (MSS). Cette vérification s'effectue par vérification de la somme de contrôle affichée de la configuration.

9.8. Personnes autorisées et procès-verbal de réception

Le test de chaque fonction SI doit être effectué par une personne autorisée et documenté dans le procès-verbal de réception après signature. Le procès-verbal de réception doit être conservé dans le journal de bord de la machine. Une personne autorisée au sens ci-dessus est une personne habilitée par le fabricant de machines **qui est capable d'effectuer de manière adéquate l'essai de réception en raison de sa formation professionnelle et de sa connaissance des fonctions de sécurité.**





Remarque

Il convient de respecter les indications et les descriptions relatives à la mise en service. Si des paramètres de fonctions SI ont été modifiés, un nouvel essai de réception doit être réalisé et ajouté au procès-verbal de réception.

Personne autorisée

Une personne autorisée peut également être un employé d'une autre entreprise chargé d'effectuer les essais si les conditions ci-dessus sont respectées. Un responsable du fabricant des machines doit toujours confirmer l'exactitude du procès-verbal de réception ; il s'agit en général du responsable de la sécurité de l'entreprise.

9.9. Contenu d'un essai de réception complet

1. Documentation

- (1) Description de la machine et image d'ensemble
- (2) Fonctions SI du programme de l'API / Impression
- (3) Description des dispositifs de sécurité
- (4) 2. Essai de fonctionnement avec vérification de chaque fonction SI utilisée
- (5) par ex. : surveillance de la porte de sécurité
- (6) par ex. : fonction d'arrêt d'urgence



3. Conclusion du procès-verbal ± Documentation contre-signatures

- (1) Contrôle de l'impression du programme
- (2) Consignation des sommes de contrôle
- (3) Vérification des sauvegardes de données
- (4) Signatures



e en service et



4. Annexe ± Enregistrements des mesures effectuées lors des essais de fonctionnement



Contenu de l'essai de réception

La réception complète d'une machine inclut également la documentation correspondante relative aux parties mécaniques, commandes, structures, processus etc. liés à la sécurité. Des dispositions très strictes s'appliquent en outre aux machines et installations soumises à une obligation de conformité aux exigences de la FDA.

9.10. Impression de sécurité

L'impression de sécurité génère une documentation relative au programme de sécurité et aide à la réception de l'installation.

L'impression de sécurité comprend :

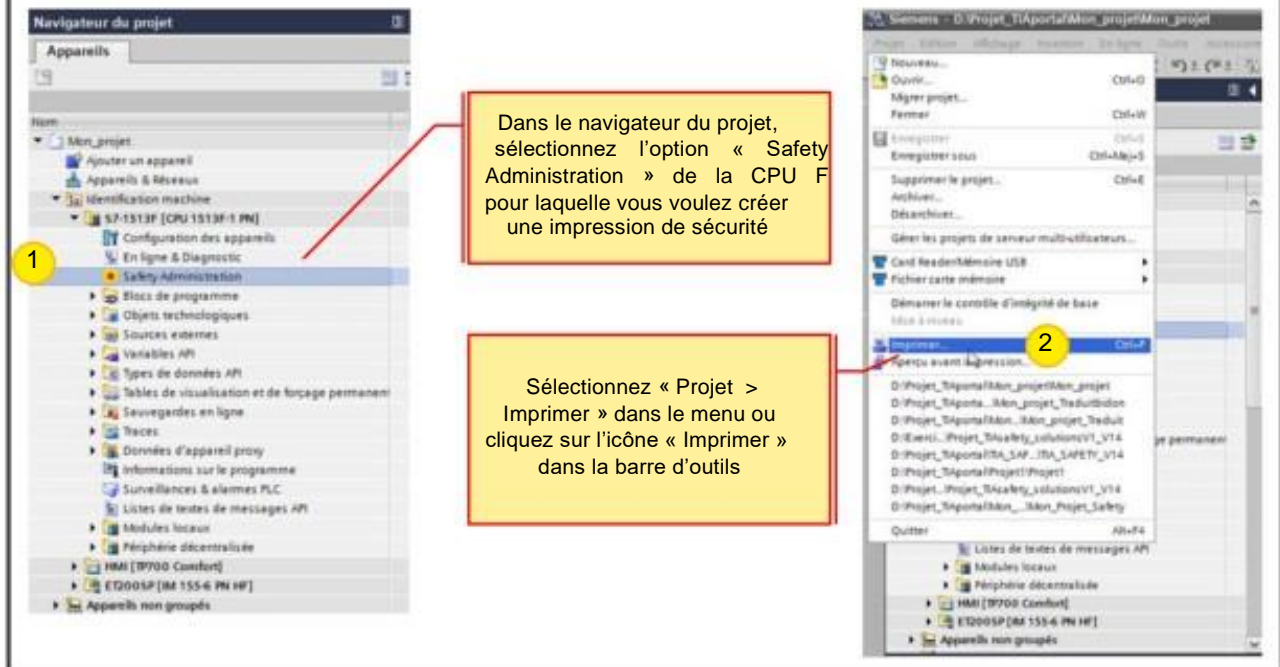
- Des informations générales pour l'identification du programme, par ex.
 - Versions logicielles utilisées
 - Signature globale F et horodatage de la génération
- Des informations sur le matériel, par ex.
 - F-CPU avec indication de la version de firmware
 - Périphérie F utilisée et son paramétrage
- Des informations sur le programme de sécurité, par ex.
 - Blocs programme utilisateur avec signature hors ligne
 - Blocs bibliothèque utilisés avec signature hors ligne

Impression de sécurité

Vous pouvez imprimer toutes les données importantes relatives à la configuration matérielle de la périphérie F et du programme de sécurité. L'impression de sécurité ainsi obtenue constitue non seulement une documentation, mais sert aussi de base à la vérification de conformité de tous les composants de l'installation. Il s'agit d'une condition préalable à la réception de l'installation. L'indication de la signature globale F dans le pied de page de l'impression garantit l'affectation correcte de l'impression à un programme de sécurité.

9.10.1. Création d'une impression de sécurité

Marche à suivre pour la création d'une impression de sécurité

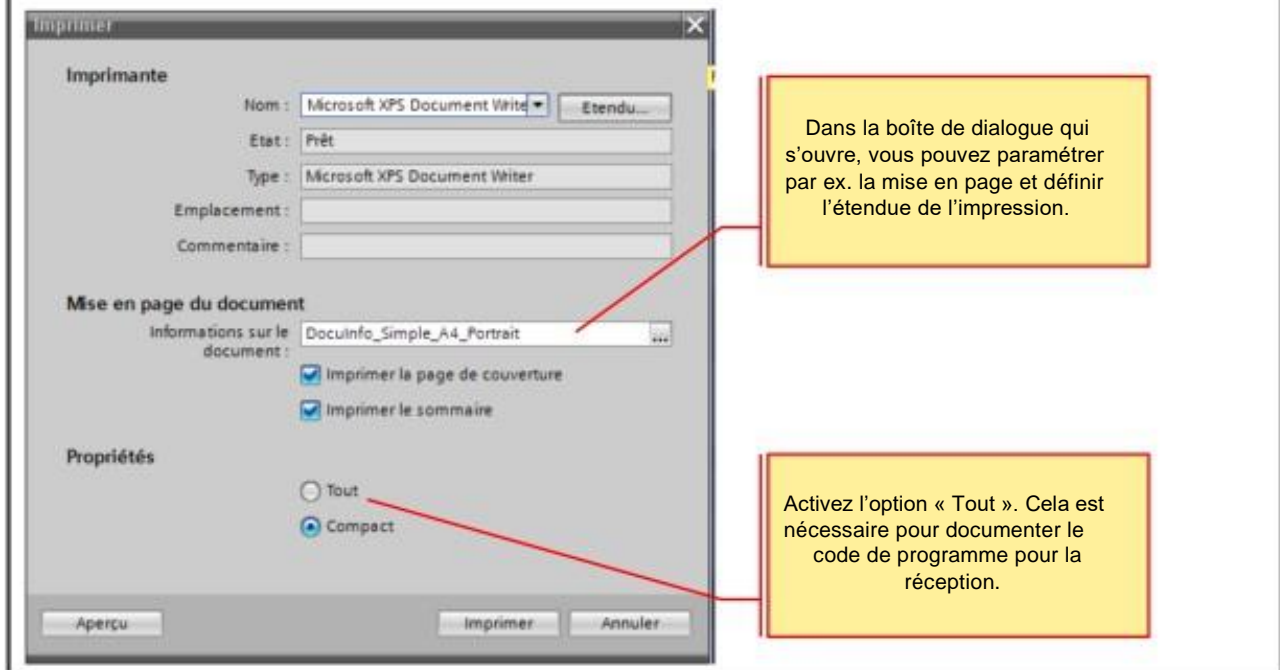


Impression de sécurité

L'impression de sécurité est la documentation du projet qui vous servira de base lors de la réception de l'installation.

9.10.2. Marche à suivre pour la création d'une impression de sécurité

Marche à suivre pour la création d'une impression de sécurité



9.10.3. Exemple d'impression de sécurité

Safety Administration

Safety Summary

General information

Collective F-signature

Collective F-signature:

Current compilation

Safety program state: The offline safety program is inconsistent.

Compilation time: 05/05/2017 16:02:25 (UTC +2:00)

Used versions

STEP 7: STEP 7 Professional V14 SP1

Safety

F-DI 8x24VDC HF_1: ET200SP, Emplacement 3

Access protection

Safety program

F-CPU

General parameters		Specific parameters	
Sensor supply 0			
Name	F-DI 8x24VDC HF_1	Short-circuit test	Yes
Emplacement	3	Time for short-circuit test	4.2 ms
Designation abrégée	F-DI 8x24VDC HF	Startup time of sensor	4.2 ms
N° d'article	RES7 136-68400-00A0	after short-circuit test	
Start address input	0	Sensor supply 1	
Start address output	0	Short-circuit test	Yes
ID address	268	Time for short-circuit test	4.2 ms
F-monitoring time	160 ms	Startup time of sensor	4.2 ms
F-source address	0	after short-circuit test	
F-destination address	0000	Sensor supply 2	
F-parameter signature (without address)	0x957E (37758)	Short-circuit test	No
F-parameter signature (with address)	0x14C4 (5316)	Time for short-circuit test	4.2 ms
Behavior after channel fault	Passivate channel	Startup time of sensor	4.2 ms
after short-circuit test		Sensor supply 3	
Short-circuit test	No	Short-circuit test	Yes
PROSafe mode	V2 mode	Time for short-circuit test	4.2 ms
PROSafe protocol version	Loop-back extension (LPE)	Startup time of sensor	4.2 ms
Version de firmware	V1.0	after short-circuit test	
Sensor supply 4			
Hardware		Short-circuit test	Yes
F-ID DB number	30003	Time for short-circuit test	4.2 ms
F-ID DB name	P00004_F-DI8x24VDC-HF_1		

Information on F-runtime group

RTG1

Safe state organization block

Name	F-ID DB (P0121)
Event class	Cyclic interrupt
Cycle time	100000 µs
Phase shift	0 µs
Priority	12
	Check whether technology objects (TDOs) are present in the user program that have a higher priority than the F-DBs. This can affect the time behavior of other CPU priority classes, including the safety program. Make sure that the safety-relevant time behavior configured in the system is not compromised.

Main safety block

Name	PC_Main_Safety (P0100)
F-ID for main safety block	-

Runtime group parameters

Name	F-runtime group 1
Max cycle time of the F-runtime group	100000 µs
Maximum cycle time of the F-runtime group	100000 µs
ID for F-runtime group communication	-
F-runtime group information DB	RTG1 (P0100)

Release 1: Schéma de câblage pour le démarrage

9.11. Réception des modifications

En cas de modifications mineures, ne testez pas de nouveau l'ensemble de l'installation, mais seulement les modifications.

La réception des modifications exige de vérifier :

- l'impact des modifications (Risk Impact Assessment) ;
- les blocs F modifiés ou ajoutés ;
- les instructions et les blocs système F modifiés ou ajoutés ;
- les paramètres de sécurité des modules de périphérie F modifiés ou ajoutés

L'évaluation d'impact (Risk Impact Assessment) permet également de définir dans quelle mesure les essais de fonctionnement doivent être répétés ou étendus.

Réception des modifications

Vous pouvez procéder à la réception des modifications de la même manière que pour la réception initiale de l'installation. Cependant, pour que vous n'ayez pas à réceptionner à nouveau l'ensemble de l'installation en cas de modifications mineures, STEP 7 Safety Advanced vous aide à identifier les parties du programme de sécurité qui ont changé. En cas de modifications, il vous suffira d'effectuer les vérifications indiquées sur la diapositive.

9.12. Exercice 1 : Réalisation d'un essai de réception

Effectuez un contrôle de fonctionnement des fonctions de sécurité d'une station partenaire à l'aide d'un « test en boîte noire ».



Réalisez en outre des simulations de défauts (tests d'injection de défauts) sur la base des résultats des analyses effectuées.

9.12.1. Exercice 1 : Description de la documentation relative à l'essai

N° d'ordre	Entrées concernées	Sorties concernées	Objet de l'essai	Conditions préalables	Description de l'essai/réalisation	Résultat attendu	Résultat de l'essai Testeur / Date
1.0			Que faut-il tester ?	Conditions préalables particulières (par ex. variations dans la configuration)	Description de l'exécution de l'essai	Quel est le résultat attendu de l'essai ?	L'essai a-t-il été concluant ?

N° d'ordre :
Un numéro d'ordre est affecté à chaque essai dans les tableaux d'essais afin de pouvoir subdiviser et numéroté précisément chaque essai.

Entrées concernées :
On indique ici, pour une meilleure vue d'ensemble, les entrées à observer lors de l'essai.

Sorties concernées :
On indique ici, pour une meilleure vue d'ensemble, les sorties à observer lors de l'essai.

Remarque : si aucune entrée ni sortie ne figurent dans cette colonne, il s'agit de signaux internes à la CPU qui doivent être observés par programme ou d'une table de variables qui doit être contrôlée.

Objet de l'essai :
On décrit ici l'objet de l'essai, c'est-à-dire ce qu'il faut tester. On indique brièvement le comportement à tester ou qui a été vérifié.

Description de l'essai/réalisation :
On explique ici la manière dont l'essai doit être exécuté ou quelle action doit être réalisée par le testeur.

Résultat attendu :
Après réalisation de l'essai, on peut vérifier ici si l'essai a été positif ou non en comparant le résultat obtenu avec le résultat attendu décrit ici.

Résultat de l'essai :
Le résultat de l'essai est complété par le testeur. On indique ici, lors de l'essai, si le résultat attendu a été atteint ou non. Si le module ou le système n'atteint pas l'objectif d'essai fixé, il convient d'en noter ici brièvement la raison.

9.12.2. Exercice 1 (suite) : Essais avant la mise en marche

Fonction	N° d'ordre	Entrées concernées	Sorties concernées	Objet de l'essai	Conditions préalables	Description de l'essai/réalisation	Résultat attendu	Résultat de l'essai Testeur / Date
Câblage	0.0			Vérification du câblage selon le schéma		On doit vérifier (contrôle visuel) que les câbles (alimentations, lignes de signaux, lignes de bus) sont correctement posés et raccordés selon le schéma	Tous les câbles sont posés et raccordés selon le schéma.	OK Eberle Thomas 01.01.2017
Fonction	N° d'ordre	Entrées concernées	Sorties concernées	Objet de l'essai	Conditions préalables	Description de l'essai/réalisation	Résultat attendu	Résultat de l'essai Testeur / Date
Redémarrage de l'installation	0.1			Redémarrage de l'installation	L'essai 0.0 doit être terminé	L'installation est mise hors tension puis remise sous tension	L'installation est prête à fonctionner (CPU en RUN, aucune SF/BF allumée)	

9.12.3. Exercice 1 (suite) : Essais en cours de service : Dispositif de levage

Fonction	N° d'ordre	Entrées concernées	Sorties concernées	Objet de l'essai	Conditions préalables	Description de l'essai/réalisation	Résultat attendu	Résultat de l'essai Testeur / Date
Arrêt d'urgence Dispositif de levage	1.0	I10.0	Q10.0 Q3.0 Q3.1	Actionnement de l'arrêt d'urgence	L'installation doit être en service et les vannes commandées en mode Automatique	Actionnement de l'arrêt d'urgence sur la cellule de vannes I10.0 1->0	La coupure du F-PM doit intervenir instantanément ; les deux vannes doivent se fermer (état de signal « 0 ») I10.0 = 0 Q10.0 = 0 Q3.0 = 0 Q3.1 = 0	
	1.1	I10.0	Q10.0 Q3.0 Q3.1	Déverrouillage de l'arrêt d'urgence	L'essai 1.0 doit être terminé	L'arrêt d'urgence est déverrouillé I10.0 0->1	Aucun redémarrage automatique ne doit intervenir I10.0 = 1 Q10.0 = 0 Q3.0 = 0 Q3.1 = 0	
	1.2	I2.3	Q10.0	Acquittement	L'essai 1.1 doit être terminé	La coupure de sécurité est acquittée via le bouton d'acquiescement I2.3 0->1	La commande des vannes est à nouveau opérationnelle I10.0 = 1 Q10.0 = 1	

9.12.4. Exercice 1 (suite) : Essais en cours de service : Etiqueteuse (1)

Fonction	N° d'ordre	Entrées concernées	Sorties concernées	Objet de l'essai	Conditions préalables	Description de l'essai/réalisation	Résultat attendu	Résultat de l'essai / Testeur / Date
Arrêt d'urgence Etiqueteuse	2.0	I22.0	Q17.0	Actionnement de l'arrêt d'urgence	L'installation doit être en service et le moteur 1 commandé	Actionnement de l'arrêt d'urgence sur le Moteur 1 I22.0 1->0	Le Moteur 1 doit être mis instantanément hors courant et tension I22.0 = 0 Q17.0 = 0	
	2.1	I22.0	Q17.0	Déverrouillage de l'arrêt d'urgence	L'essai 2.0 doit être terminé	L'arrêt d'urgence est déverrouillé puis la commande bimanuelle actionnée I22.0 0->1	Aucun redémarrage automatique ne doit intervenir I22.0 = 1 Q17.0 = 0	
	2.2	I2.3	Q17.0	Acquittement	L'essai 2.1 doit être terminé	La coupure de sécurité est acquittée via le bouton d'acquiescement et la commande bimanuelle actionnée I2.3 0->1	La commande du Moteur 1 est à nouveau opérationnelle I22.0 = 1 Q17.0 = 1	

9.12.5. Exercice 1 (suite) : Essais en cours de service : Etiqueteuse (2)

Fonction	N° d'ordre	Entrées concernées	Sorties concernées	Objet de l'essai	Conditions préalables	Description de l'essai/ réalisation	Résultat attendu	Résultat de l'essai Testeur / Date
Surveillance commande bimanuelle Etiqueteuse	3.0	I22.2 I22.6	Q17.0	Surveillance bimanuelle à l'intérieur de la discordance	L'installation doit être en service. Le Moteur 1 ne doit pas être enclenché Q17.0 = 0	Actionnement des boutons S1 et S2 à l'intérieur du délai de discordance de 200 ms I22.2 0->1 I22.6 0->1	Le Moteur 1 est commandé I22.2 = 1 I22.6 = 1 Q17.0 = 1	
	3.1	I22.2 I22.6	Q17.0	Surveillance bimanuelle en dehors de la discordance (S1 intervient trop tard)	L'installation doit être en service. Le Moteur 1 ne doit pas être enclenché Q17.0 = 0	Actionnement du bouton S2 et après la discordance, actionnement du bouton S1 I22.6 0->1 Attente : > 200 ms I22.2 0->1	Le Moteur 1 n'est pas commandé I22.2 = 1 I22.6 = 1 Q17.0 = 0	
	3.2	I22.2 I22.6	Q17.0	Surveillance bimanuelle en dehors de la discordance (S2 intervient trop tard)	L'installation doit être en service. Le Moteur 1 ne doit pas être enclenché Q17.0 = 0	Actionnement du bouton S1 et après la discordance paramétrée, actionnement du bouton S2 I22.2 0->1 Attente : > 200 ms I22.6 0->1	Le Moteur 1 n'est pas commandé I22.2 = 1 I22.6 = 1 Q17.0 = 0	

9.12.6. Exercice 1 (suite) : Essais en cours de service : Robot Mode automatique (1)

Fonction	N° d'ordre	Entrées concernées	Sorties concernées	Objet de l'essai	Conditions préalables	Description de l'essai/ réalisation	Résultat attendu	Résultat de l'essai Testeur / Date
Arrêt d'urgence Robot Mode automatique	4.0	I4.1	Q17.1	Actionnement de l'arrêt d'urgence	L'installation doit être en mode automatique et le Moteur 2 commandé	Actionnement de l'arrêt d'urgence sur le Moteur 2 I4.1 1->0	Le Moteur 2 doit être mis instantanément hors courant et tension I4.1 = 0 Q17.1 = 0	
	4.1	I4.1	Q17.1	Déverrouillage de l'arrêt d'urgence	L'essai 4.0 doit être terminé	L'arrêt d'urgence est déverrouillé I4.1 0->1	Aucun redémarrage automatique ne doit intervenir I4.1 = 1 Q17.1 = 0	
	4.2	I2.3	Q17.1	Acquittement	L'essai 4.1 doit être terminé	La coupure de sécurité est acquittée via le bouton d'acquiescement I2.3 0->1	La commande du Moteur 2 est à nouveau opérationnelle I4.1 = 1 Q17.1 = 1	

9.12.7. Exercice 1 (suite) : Essais en cours de service : Robot Mode automatique (2)

Fonction	N° d'ordre	Entrées concernées	Sorties concernées	Objet de l'essai	Conditions préalables	Description de l'essai / réalisation	Résultat attendu	Résultat de l'essai / Testeur / Date
Surveillance Porte de sécurité	5.0	I22.1	Q17.1	Ouverture de la porte de sécurité	L'installation doit être en mode automatique et le Moteur 2 commandé	Ouverture de la porte de sécurité I22.1 1->0	Le Moteur 2 doit être mis instantanément hors courant et tension I22.1 = 0 Q17.1 = 0	
	5.1	I22.1	Q17.1	Fermeture de la porte de sécurité	L'essai 5.0 doit être terminé	Refermeture de la porte de sécurité I22.1 0->1	Aucun redémarrage automatique ne doit intervenir I22.1 = 1 Q17.1 = 0	
	5.2	I2.3	Q17.1	Acquittement	L'essai 5.1 doit être terminé	La coupure de sécurité est acquittée via la bouton d'acquiescement I2.3 0->1	La commande du Moteur 2 est à nouveau opérationnelle I22.1 = 1 Q17.1 = 1	

9.12.8. Exercice 1 (suite) : Essais en cours de service : Robot Mode maintenance

Fonction	N° d'ordre	Entrées concernées	Sorties concernées	Objet de l'essai	Conditions préalables	Description de l'essai/réalisation	Résultat attendu	Résultat de l'essai Testeur / Date
Arrêt d'urgence Robot Mode maintenance	6.0	I4.1	Q17.1	Actionnement de l'arrêt d'urgence	L'installation doit être en mode maintenance et le Moteur 2 commandé	Actionnement de l'arrêt d'urgence sur le Moteur 2 I4.1 1->0	Le Moteur 2 doit être mis instantanément hors courant et tension I4.1 = 0 Q17.1 = 0	
	6.1	I4.1	Q17.1	Déverrouillage de l'arrêt d'urgence	L'essai 6.0 doit être terminé	L'arrêt d'urgence est déverrouillé I4.1 0->1	Aucun redémarrage automatique ne doit intervenir I4.1 = 1 Q17.1 = 0	
	6.2	I2.3	Q17.1	Acquittement	L'essai 6.1 doit être terminé	La coupure de sécurité est acquittée via le bouton d'acquiescement I2.3 0->1	La commande du Moteur 2 est à nouveau opérationnelle I4.1 = 1 Q17.1 = 1	

9.12.9. Exercice 1 (suite) : Essais en cours de service : Test d'injection de défauts

Fonction	N° d'ordre	Entrées concernées	Sorties concernées	Objet de l'essai	Conditions préalables	Description de l'essai/réalisation	Résultat attendu	Résultat de l'essai Testeur / Date
Court-circuit sur l'arrêt d'urgence	7.0	I4.1	Q17.1	Actionnement du commutateur de court-circuit	L'installation doit être en service et le Moteur 2 commandé	Actionnement du commutateur de court-circuit	Le Moteur 2 doit être instantanément mis hors courant et tension I4.1 = 0 Q17.1 = 0	
	7.1	I4.1	Q17.1	Déverrouillage du commutateur de court-circuit	L'essai 7.0 doit être terminé	Le commutateur de court-circuit est déverrouillé	Aucun redémarrage automatique ni dépassivation ne doivent intervenir E4.1 = 0 A17.1 = 0	
	7.2	I2.3	Q17.1	Acquittement périphérie	L'essai 7.1 doit être terminé	Le défaut du canal est acquitté via le bouton d'acquittement I2.3 0->1	Aucun redémarrage automatique ne doit intervenir I4.1 = 1 Q17.1 = 0	
	7.3	I2.3	Q17.1	Acquittement arrêt d'urgence	L'essai 7.2 doit être terminé	La coupure de sécurité est acquittée via le bouton d'acquittement I2.3 0->1	La commande du Moteur 2 est à nouveau opérationnelle I4.1 = 1 Q17.1 = 1	

9.12.10. Exercice 1 (suite) : Résultat

Résumé de l'essai

Constatations

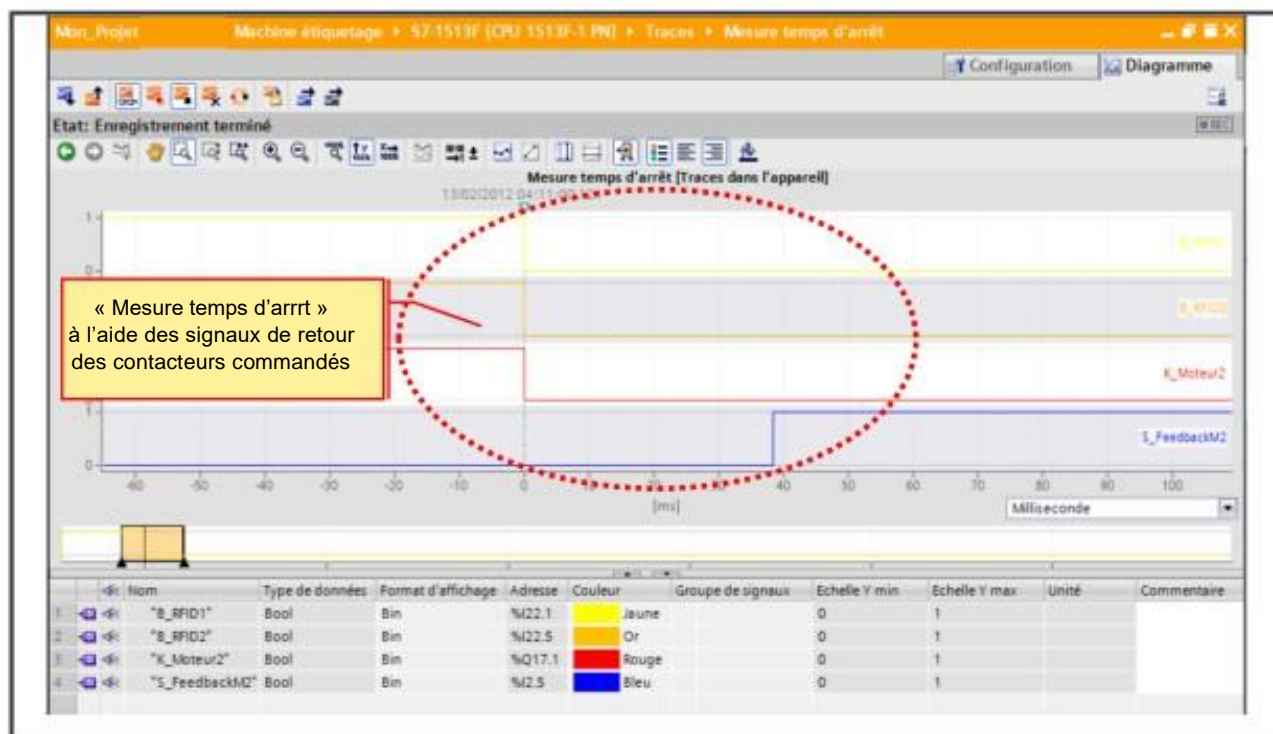
Constatations primaires (exigences non satisfaites)

Constatations secondaires (exigences partiellement satisfaites)

Remarques (exigences satisfaites)

Résumé

9.13. Exercice 2 : « Mesure temps d'arrêt » Moteur 2 via Trace



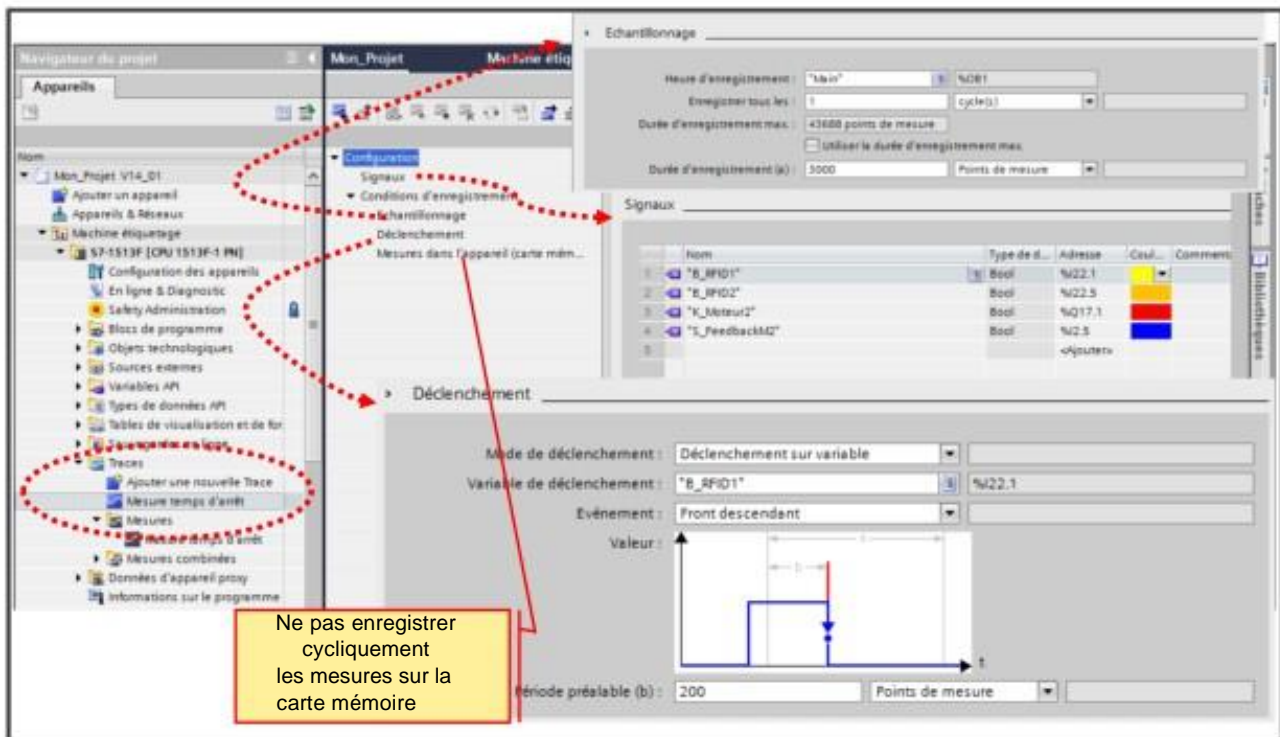
Enoncé

On veut effectuer une « Mesure du temps d'arrêt » du Moteur 2. On évalue pour ce faire les signaux de retour (« S_FeedbackM2 ») des contacteurs lors d'une coupure du Moteur 2. Vous devez déterminer le temps qu'il faut au signal de retour (« S_FeedbackM2 ») pour changer d'état après une coupure du Moteur 2. La coupure doit être provoquée par l'ouverture de la porte de sécurité en Mode automatique.

Marche à suivre

Suite à la page suivante

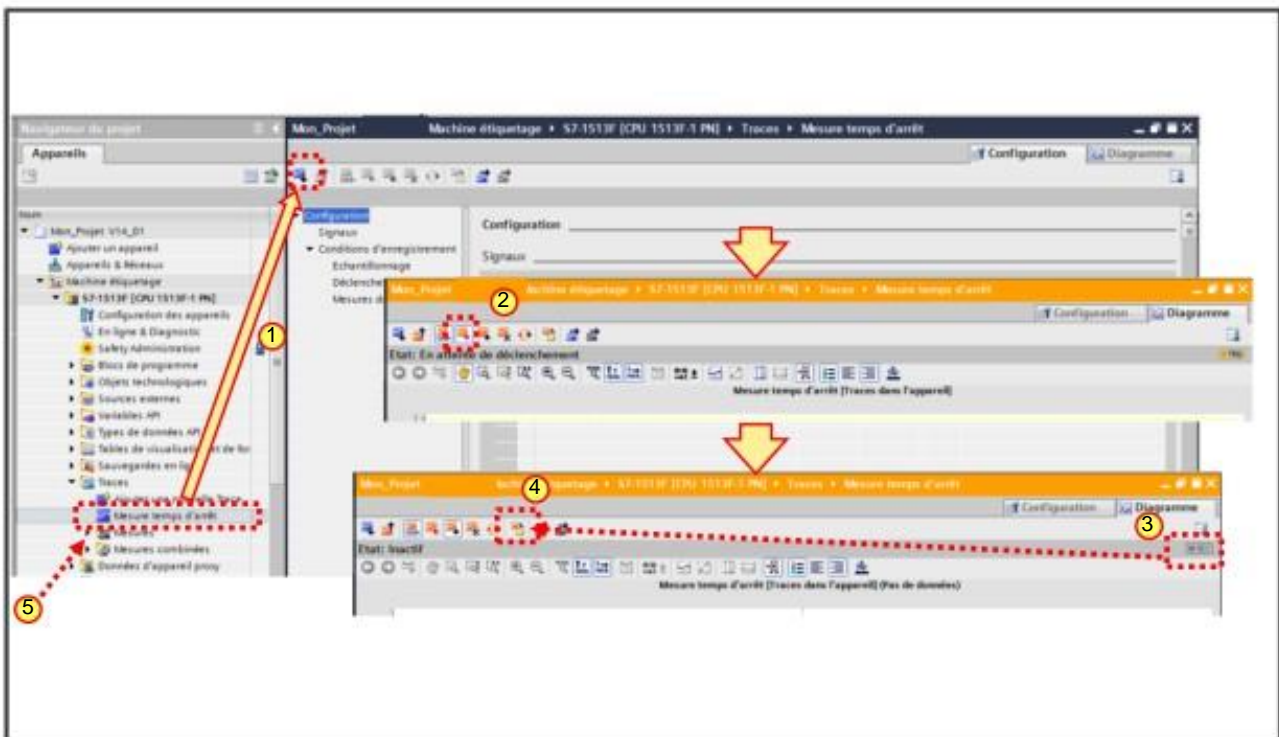
9.13.1. Exercice 2 (suite) : Créer une Trace



Marche à suivre

1. Créez une Trace nommée « Mesure temps d'arrêt »
2. Sélectionnez les signaux que vous voulez observer (voir diapositive)
3. Choisissez un échantillonnage et une variable de déclenchement appropriés (voir diapositive)
4. Enregistrez votre projet

9.13.2. Exercice 2 (suite) : Charger, démarrer et enregistrer une Trace



Marche à suivre

1. Chargez la Trace dans la CPU
2. Activez l'enregistrement. L'enregistrement s'effectuera alors de manière temporaire dans une mémoire tampon circulaire.
3. Après l'activation, l'enregistrement est en attente de déclenchement (TRIG=jaune). Après déclenchement de la variable, l'enregistrement démarre (REC=rouge). Attendez que l'enregistrement soit terminé (REC=gris).
4. La mesure est maintenant disponible en ligne sur la CPU et doit être enregistrée dans le projet hors ligne pour être évaluée.
5. Analysez la mesure et déterminez le « temps d'arrêt » sur la base du signal de retour.

Table des matières

10. Maintenance et diagnostic	10-2
10.1. Diagnostic général	10-3
10.2. LED de signalisation	10-4
10.3. Signification des LED (1)	10-5
10.4. Signification des LED (2)	10-6
10.5. Extensions de l'affichage sur les CPU S7-1500F	10-7
10.6. Marche à suivre pour le diagnostic d'erreurs ayant une incidence sur la sécurité (1).....	10-8
10.7. Marche à suivre pour le diagnostic d'erreurs ayant une incidence sur la sécurité (2).....	10-9
10.8. Chargement cohérent de projets de sécurité.....	10-10
10.9. TIA Portal - Compatibilité en ligne.....	10-11
10.10. Exercice : Recherche d'erreurs.....	10-12
10.10.1. Exercice 1 : Chargement du Service Projet (CPU+IHM) dans les appareils	10-13
10.10.2. Exercice 2 : Assignez à l'ET200SP un nom En Ligne.....	10-14
10.10.3. Exercice 3 : STOP - Recherche d'erreurs	10-15
10.10.4. Solution : Erreurs sur modules	10-17
10.10.5. Solution : Erreurs fonctionnelles.....	10-18

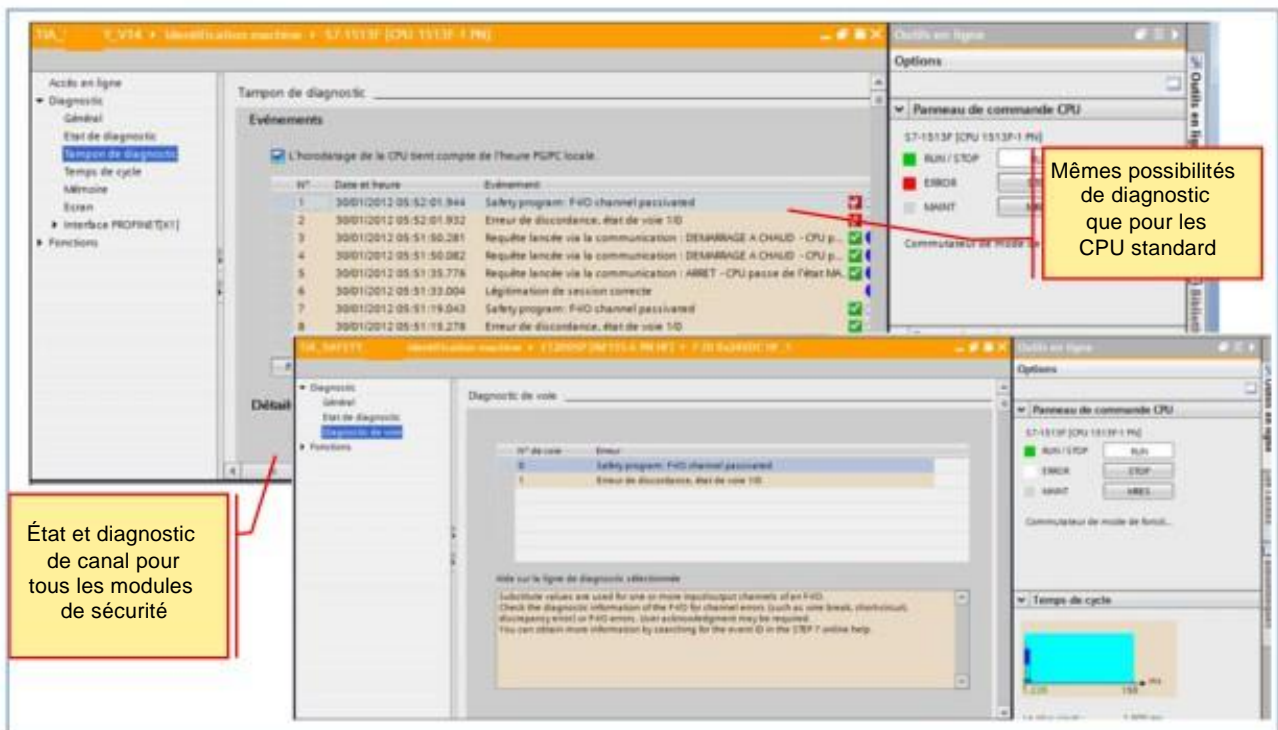
10. Maintenance et diagnostic

À l'issue de la formation, le participant au stage saura

- ... interpréter les LED des modules de sécurité
- ... commander l'affichage sur les CPU 1500F
- ... identifier les erreurs/défauts, comprendre les messages de diagnostic et les éliminer
- ... remplacer un module et effectuer une mise à jour du microprogramme



10.1. Diagnostic général



Diagnostic système

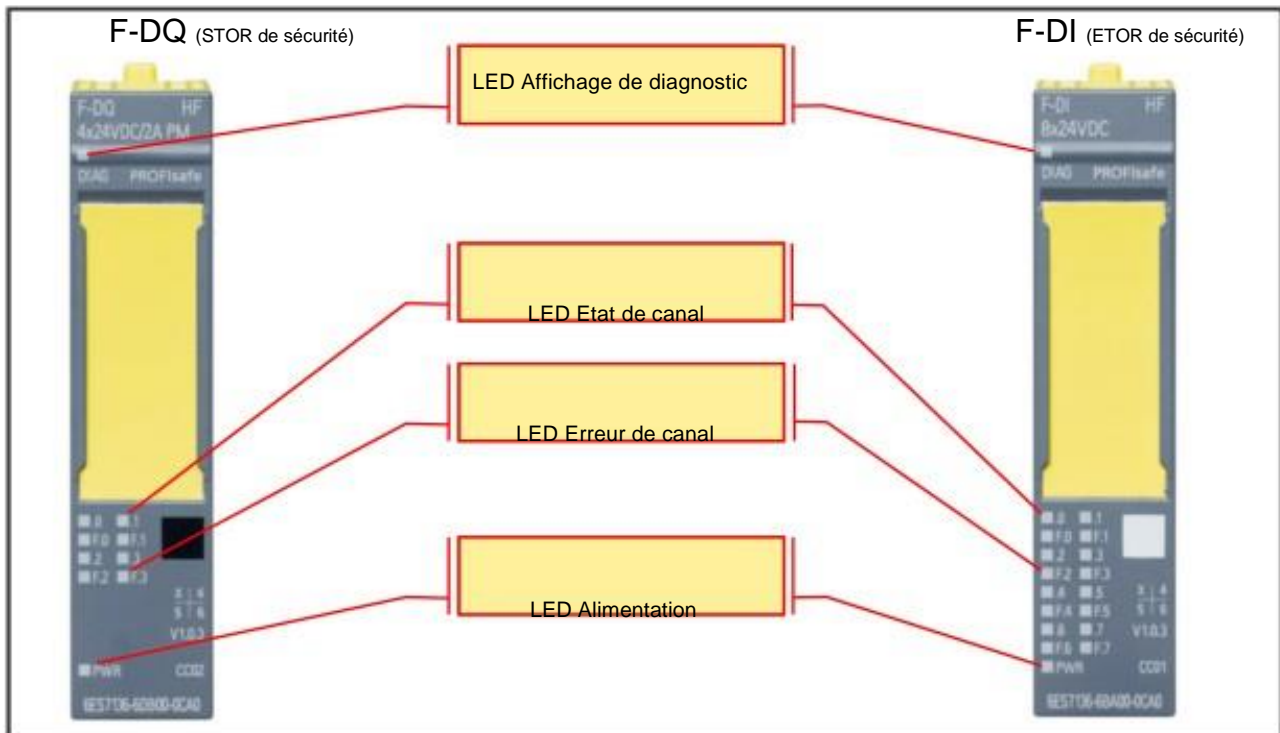
Tous les produits SIMATIC intègrent des fonctions de diagnostic qui permettent de détecter et d'éliminer les erreurs. Les composants signalent automatiquement les dysfonctionnements éventuels et fournissent des informations détaillées supplémentaires. Un diagnostic à l'échelle de l'installation vous permet de minimiser les temps d'arrêt non planifiés. Le système d'automatisation SIMATIC surveille les états suivants dans l'installation en cours de fonctionnement :

- Défaillance/rétablissement d'un appareil
- Événement de débrogage/enfichage
- Erreur de module
- Erreur d'accès à la périphérie
- Erreur de canal
- Erreur de paramétrage
- Défaillance de la tension auxiliaire externe

Messages de diagnostic

Les erreurs de module sont affichées en tant que diagnostics (état du module). Une fois les erreurs éliminées, vous devez réintégrer le module F dans le programme de sécurité.


10.2. LED de signalisation




La LED DIAG et les LED d'état de canal et d'erreur de canal des entrées ne répondent pas aux critères requis pour les applications de sécurité. Elles ne doivent donc pas être évaluées en liaison avec des fonctions de sécurité.

10.3. Signification des LED (1)

F-DQ (STOR de sécurité)



F-DI (ETOR de sécurité)











LED DIAG	Signification
■ éteinte	Alimentation du bus interne de l'ET 200SP défectueuse
■ clignote	Module non paramétré
■ allumée	Module paramétré, pas de diagnostic du module
■ clignote	Module paramétré et diagnostic du module







LED PWR	Signification
■ éteinte	Tension d'alimentation L+ absente
■ allumée	Tension d'alimentation L+ appliquée

10.4. Signification des LED (2)


F-DQ (STOR de sécurité)



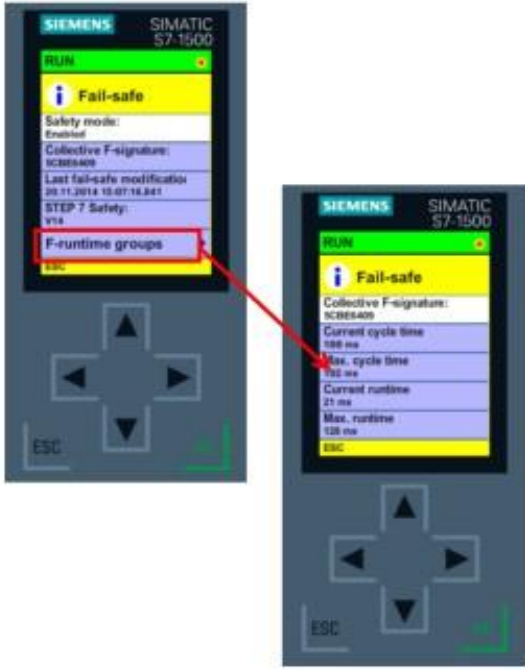
Etat de la voie	Erreur de voie	Description
 désactivée	 désactivée	Signal de process = 0 et pas de diagnostic de voie
 activée	 désactivée	Signal de process = 1 et pas de diagnostic de voie
 désactivée	 activée	Signal de process = 0 et diagnostic de voie
 clignotent alternativement		<ul style="list-style-type: none">Utilisation avec des CPU F S7-1200/1500 : une voie au moins attend l'acquittement de l'utilisateur.Utilisation avec des CPU F S7-300/400 : une voie au moins attend l'acquittement de l'utilisateur.

Etat de la voie	DIAG	Erreur de voie	Description
 désactivée	 clignote	 Toutes activées	L'adresse PROFIsafe ne correspond pas à l'adresse PROFIsafe de la configuration.
 clignote	 clignote	 désactivée	Identification du module F lors de l'attribution de l'adresse PROFIsafe

F-DI (ETOR de sécurité)



10.5. Extensions de l'affichage sur les CPU S7-1500F



Les CPU S7-1500F avec affichage affichent les informations suivantes dans le menu « Aperçu », rubrique « Sécurité » :

- Mode de sécurité activé/désactivé ➤
- Signature globale F
- Dernière modification de sécurité
- Version de STEP 7 Safety avec lequel le programme de sécurité a été compilé
- Informations sur les groupes d'exécution F (RTGSYSInfo)

Pour chaque périphérie F, les informations suivantes s'affichent dans le menu « Etat », rubrique « Sécurité » :

- Signature des paramètres F (avec adresse) ➤
- Mode de sécurité
- Temps de surveillance F
- Adresse source F
- Adresse cible F

10.6. Marche à suivre pour le diagnostic d'erreurs ayant une incidence sur la sécurité (1)

COMMENT se manifeste l'erreur ?

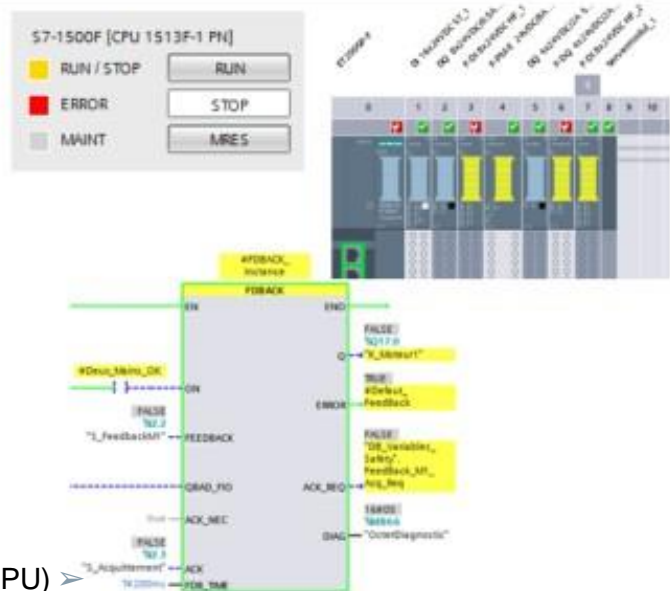
- Erreur détectée par le système (erreur module, dépassement cycle)
- Erreur fonctionnelle (erreur logique, déclenchement d'une fonction de sécurité)

OÙ se manifeste l'erreur ?

- dans le programme (blocs de sécurité)
- sur modules de sécurité individuels ➤
- sur des stations complètes

QUAND se manifeste l'erreur ?

- En permanence (dès le démarrage de la CPU) ➤
- Sporadiquement (à intervalles indéfinis)
- A certains changements de signaux (par ex. signal d'entrée spécial)



10.7. Marche à suivre pour le diagnostic d'erreurs ayant une incidence sur la sécurité (2)

Recherche d'erreurs

1. Même procédure que pour un diagnostic standard

Examiner les messages de diagnostic

- Vérifier le paramétrage
- Vérifier le câblage

2. Procédure spéciale pour les erreurs ayant une incidence sur la sécurité

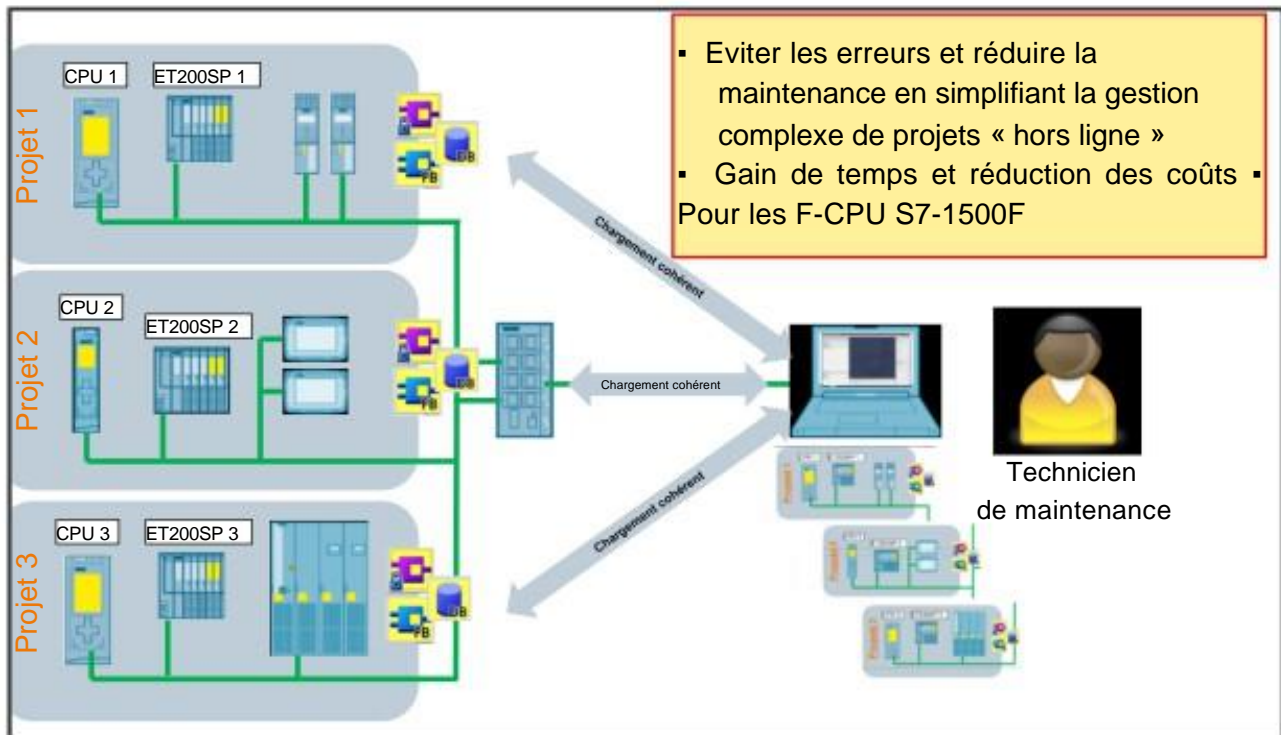
- Dépassement du temps de surveillance :
 - Vérifier le temps de surveillance PROFIsafe des modules
- Erreur de paramétrage :
 - Vérifier les adresses cibles et les éléments de codage des modules F ➤

Altération des données, erreur CRC :

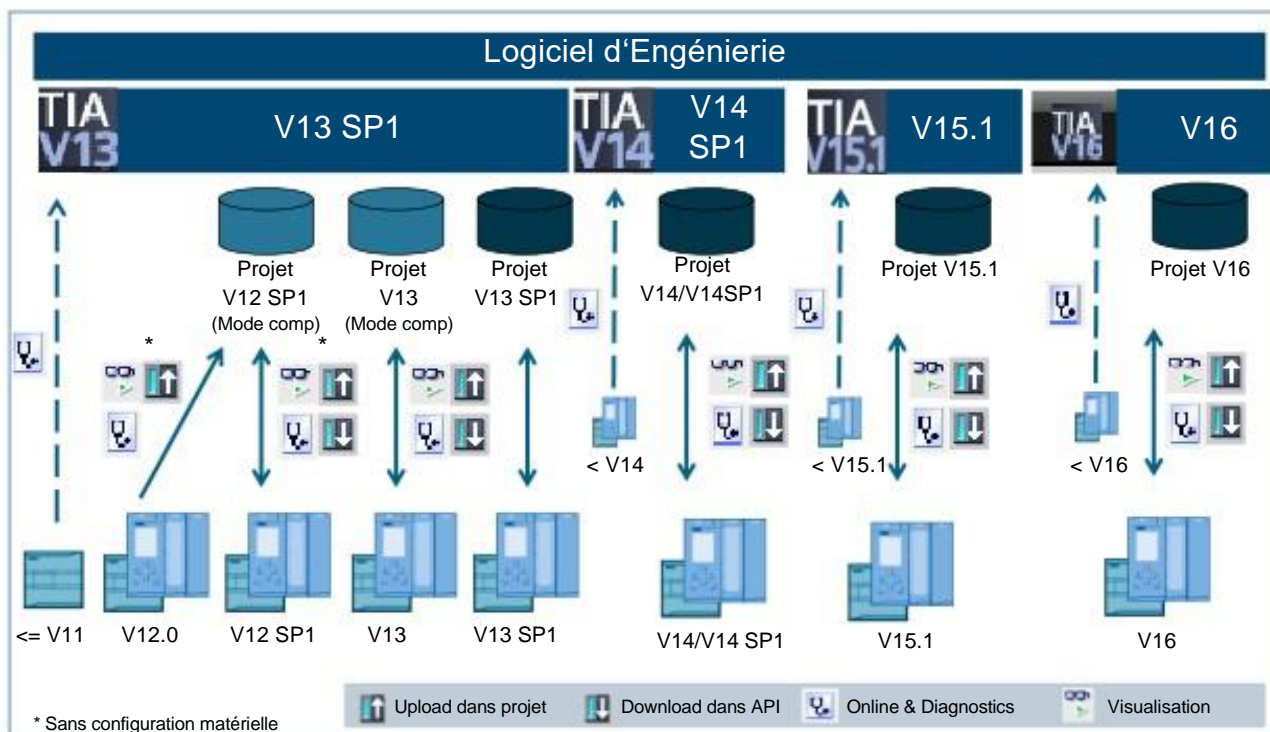
- Ne pas exécuter le programme standard pour détecter d'éventuels accès interdits
- Bloquer la communication standard pour détecter d'éventuels accès interdits



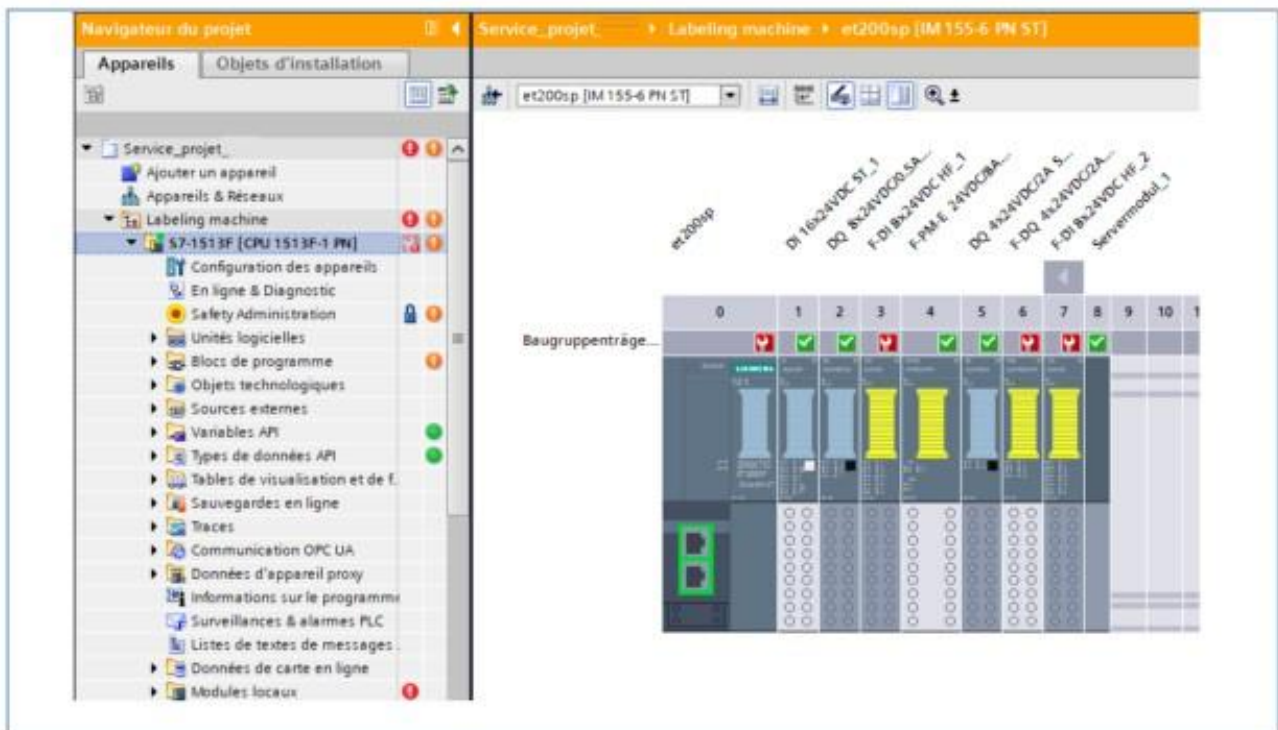
10.8. Chargement cohérent de projets de sécurité



10.9. TIA Portal - Compatibilité en ligne



10.10. Exercice : Recherche d'erreurs



Énoncé

On veut à présent simuler un cas de maintenance classique. Vous êtes un technicien de maintenance et vous vous rendez sur le site d'un client. L'installation est en panne. Vous devez rechercher l'ensemble des erreurs/défauts/dysfonctionnements et les éliminer afin que l'installation puisse redémarrer.

Procédure

Voir page suivante

10.10.1. Exercice 1 : Chargement du Service Projet (CPU+IHM) dans les appareils.

Vous trouverez le projet sur votre PG :
D:\Exercices_TIA_Portal_V16\TIA_SAFETY\Service_projet_V16.zap16

Chargez la CPU et l'IHM

Énoncé

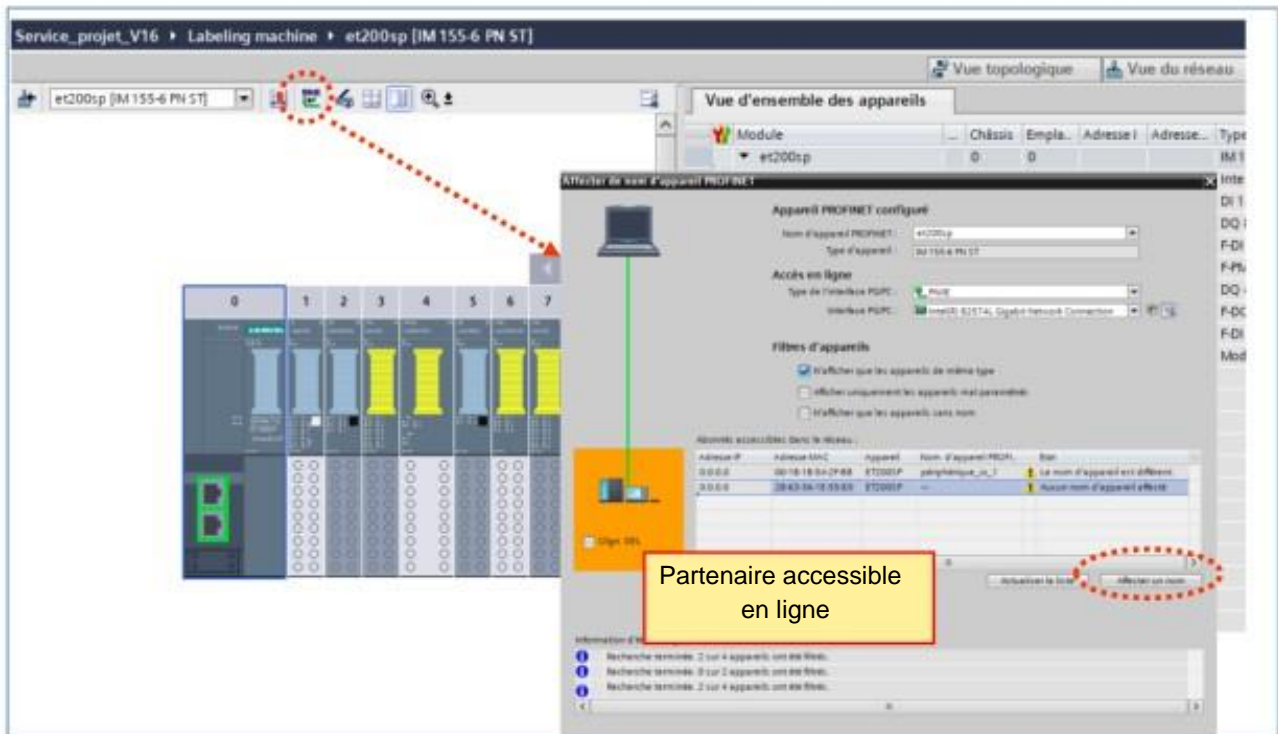
Pour effectuer la recherche d'erreurs, vous devez d'abord charger un projet défectueux dans l'installation. Vous trouverez à cet effet un projet sous « D:\Exercices_TIA_Portal_V16\TIA-SAFETY\Service_projet_V16 ».

Le projet ne présente pas de protection. En exploitation il faudra toujours protéger la CPU et le programme de sécurité (protection Hors Ligne et En Ligne)

Procédure

1. Ouvrez le projet
2. Charger la CPU et l'IHM.

10.10.2. Exercice 2 : Assignez à l'ET200SP un nom En Ligne.



Énoncé

Le nom d'appareil PROFINET doit être affecté En ligne à l'ET200SP. Le contrôleur affectera ainsi l'adresse IP paramétrée Hors ligne lors de son démarrage.

Procédure

1. Retenez la vue de l'appareil ET200SP.
2. Par clic droit sur l'IM accédez à « Affecter un nom d'appareil ».
3. Vérifiez le nom d'appareil configuré.
4. Retenez l'interface de liaison et actualisez la liste des abonnés
5. Retenez l'ET200SP et activez « Affecter un nom »
6. Enregistrez votre projet.

Résultat

La CPU est en RUN et la led rouge ERROR clignote. L'ET 200SP est paramétré.

La led RN (RUN) de l'IM est permanente. Des modules signalent un défaut/diagnostic via la led DIAG

10.10.3. Exercice 3 : STOP - Recherche d'erreurs

Énoncé

Le projet de maintenance contient deux types d'erreurs :

1. 3 erreurs système (erreurs détectées par le système)
2. 3 erreurs de fonctionnement (erreurs non détectées par le système)

Commencez par rechercher et éliminer toutes les erreurs système. Localisez ensuite toutes les erreurs de fonctionnement et éliminez-les. Le fonctionnement correct de l'installation est identique à celui décrit dans les exercices de programmation

Procédure : Rechercher et éliminer les erreurs système

À l'aide des possibilités de diagnostic en ligne (tampon de diagnostic, état du module, diagnostic de canal, etc.), recherchez et éliminez toutes les erreurs système.

- Première erreur :

– Erreur



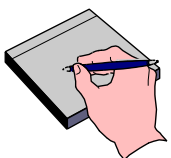
–
.....

– Correction :

–
.....

- Deuxième erreur :

– Erreur



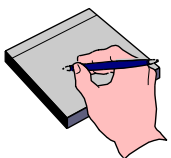
–
.....

– Correction :

–
.....

- Troisième erreur :

– Erreur



–
.....

– Correction :

–
.....

Procédure : Rechercher et éliminer les erreurs de fonctionnement

À l'aide des fonctions de diagnostic (visualiser le module, tables de visualisation, octet de diagnostic des fonctions de sécurité, etc.), recherchez et éliminez toutes les erreurs de fonctionnement.



- Première erreur :
Les vannes d'arrêt ne peuvent plus être coupées via l'arrêt d'urgence local « E3 »

– Erreur

–
.....

– Correction :

–
.....



- Deuxième erreur :
Le Moteur 1 ne peut plus être commandé via la commande bimanuelle

– Erreur

–
.....

– Correction :

–
.....



- Troisième erreur :
Le Moteur 2 ne peut plus être commandé en mode automatique et en mode maintenance

– Erreur

–
.....

– Correction :

–
.....

10.10.4. Solution : Erreurs sur modules

Erreur	Cause	Correction
1	Les signaux de l'arrêt d'urgence E2 sont mal évalués (F-DI empl. 3 Paire de canaux 3,7 = 1oo2 antivalent)	1oo2 antivalent → 1oo2 équivalent
2	L'adresse PROFIsafe (adresse cible F) est mal paramétrée (F-DO empl. 6)	Réattribuer l'adresse PROFIsafe
3	Le temps de surveillance F est réglé à une valeur trop basse (F-DI empl. 7)	Temps de surveillance F 80 ms → 150 ms

10.10.5. Solution : Erreurs fonctionnelles



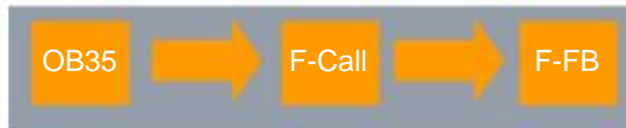
Erreur	Cause	Correction
1	Les signaux de l'arrêt d'urgence local (E3) et global (E2) sont traités avec l'instruction OR -> FB-Lifting	Instruction OR  instruction AND
2	TWO_H_EN ne fonctionne pas, le diagnostic du bloc fournit le code 16#01 (temps de discordance mal paramétré) -> FB-Labeling	Réattribuer l'adresse PROFIsafe
3	Le démarrage du moteur 2 provoque immédiatement une erreur de relecture dans le bloc FBACK (ERROR=1) Le diagnostic du bloc fournit l'erreur 16#41 (Temps de relecture trop court) -> FB-Robot	FDB_TIME 0 ms  100 ms (> 0ms)

Table des matières

11. Annexe : Migration d'un programme de sécurité	11-2
11.1. Migration de Distributed Safety vers STEP 7 Safety	11-3
11.1.1. Changement dans la structure du programme	11-3
11.1.2. Recette technique	11-4
11.1.3. Signature.....	11-5
11.1.4. Téléchargement sans modification	11-6
11.1.5. Nouvelle compilation du programme	11-7
11.1.6. Versions du programme de sécurité (1)	11-8
11.1.7. Versions du programme de sécurité (2)	11-9
11.2. Migration de S7-300F vers S7-1500F	11-10
11.2.1. Instructions non admissibles.....	11-11
11.2.2. Modification de la programmation.....	11-12
11.2.3. Modification des fonctions de sécurité (1)	11-13
11.2.4. Modification des fonctions de sécurité (2)	11-14
11.3. Mettre à niveau des projets STEP 7 Safety V13 SP1 en V16	11-15
11.3.1. Nouvelle compilation	11-16
11.3.2. F-Convert-Log	11-17
11.4. Mettre à niveau des projets STEP 7 Safety antérieurs à V13 SP1	11-18

11. Annexe : Migration d'un programme de sécurité

Les projets réalisés sous S7 Distributed Safety V5.4 SP5 peuvent continuer à être utilisés dans STEP 7 Safety Advanced V16.



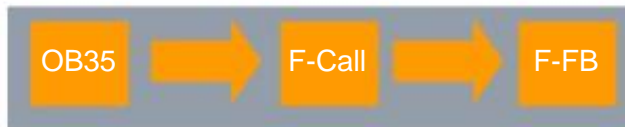
Remarque : Le programme de sécurité est compilé uniquement si le mot de passe du programme de sécurité a été saisi. Sans saisie du mot de passe, seul le programme utilisateur standard sera compilé.



11.1. Migration de Distributed Safety vers STEP 7 Safety

11.1.1. Changement dans la structure du programme

Les projets réalisés sous S7 Distributed Safety V5.4 SP5 peuvent continuer à être utilisés dans STEP 7 Safety Advanced V16.



Remarque : Le programme de sécurité est compilé uniquement si le mot de passe du programme de sécurité a été saisi. Sans saisie du mot de passe, seul le programme utilisateur standard sera compilé.



Migration des projets S7 Distributed Safety V5.4 SP5 vers STEP 7 Safety Advanced V16

Dans STEP 7 Safety Advanced V16, vous pouvez continuer à utiliser les projets comportant des programmes de sécurité qui ont été créés avec S7 Distributed Safety V5.4 SP5. Pour cela, vous devez avoir compilé les projets dans S7 Distributed Safety V5.4 SP5, puis les faire migrer.

11.1.2. Recette technique

L'opération de migration permet de créer un projet STEP 7 Safety complet avec un programme de sécurité dans lequel [la structure du programme S7 Distributed Safety et la signature globale](#) ont été [conservées](#).

Le projet migré [ne nécessite pas de nouvelle réception \(recette technique\)](#) et peut être directement chargé dans la CPU de sécurité sans nouvelle compilation.

L'édition du projet qui a été réalisé sous S7 Distributed Safety V5.4 SP5 et les dossiers de réception (impression) restent valides.

Ce n'est que lors de la [recompilation](#) du projet migré avec STEP7 Safety Advanced V16 que lui sont attribuées la [nouvelle structure du programme et une nouvelle signature globale](#).

Après la migration

Les blocs de sécurité de la bibliothèque F S7 Distributed Safety (V1) sont convertis en instructions pouvant être utilisées par STEP 7 Safety Advanced. Le projet migré ne doit pas faire l'objet d'une recette technique et peut être chargé dans la CPU F sans être modifié, dans la mesure où il n'est pas retravaillé après la migration.

Impression de sécurité

Vous ne pouvez pas sortir une impression du programme de sécurité dans STEP 7 Safety Advanced pour un projet migré. L'impression du projet créé avec S7 Distributed Safety V5.4 SP5, ainsi que les documents de réception associés, restent valides car la signature globale sécurisée a été conservée.

Remarque

Après la migration d'un SM 326 ; DI 24 x 24 VCC (6ES7 326-1BK01-0AB0 et 6ES7 326-1BK02-0AB0), le message d'erreur suivant peut apparaître lors de la compilation de la configuration matérielle : « F_IPParam_ID_1: valeur hors de la plage admissible ».

Solution :

Supprimez le module et réinsérez-le. Le message d'erreur « Erreur interne lors du calcul CRC. Le CRC (F_Par_CRC) du module (x) ne correspond pas à la valeur calculée (y). » est une erreur consécutive à cette opération et disparaîtra à la suppression de la cause.

11.1.3. Signature

Téléchargement du projet migré sans modification

La signature du projet migré correspond à celle du projet d'origine.

- Boîte de dialogue Distributed Safety :



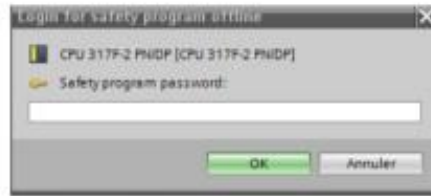
- Boîte de dialogue Safety Advanced V16 :



11.1.4. Téléchargement sans modification

Téléchargement du projet migré sans modification

Le mot de passe du programme de sécurité ne doit pas être saisi lors de la compilation du projet.



Ne pas saisir le mot de passe

Saisir le mot de passe

11.1.5. Nouvelle compilation du programme

Compilation du projet migré

Après la compilation du programme de sécurité, la structure et la signature du programme de sécurité changent.

- Avant la compilation :



Offline signature	Time stamp
73549B11	3/5/2014 7:57:56 PM (UTC +1:00)

- Après la compilation :



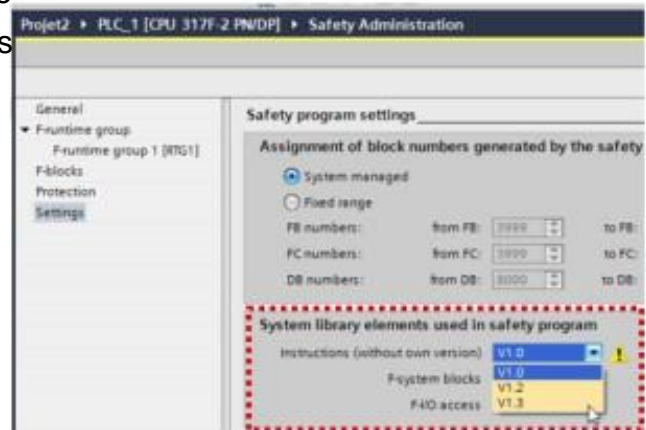
Offline signature	Time stamp
9AB138AF	3/5/2014 9:18:01 PM (UTC +1:00)

11.1.6. Versions du programme de sécurité (1)

Recommandation lors de la modification du programme de sécurité :

Avant la première compilation avec STEP 7 Safety Advanced V16, les éléments de la bibliothèque système utilisés dans le programme de sécurité doivent être convertis dans la version la plus récente disponible.

Le paramètre de conversion peut être modifié dans Safety Administration, rubrique « Paramètres » (Settings).



Dernière version des éléments de la bibliothèque dans le programme de sécurité

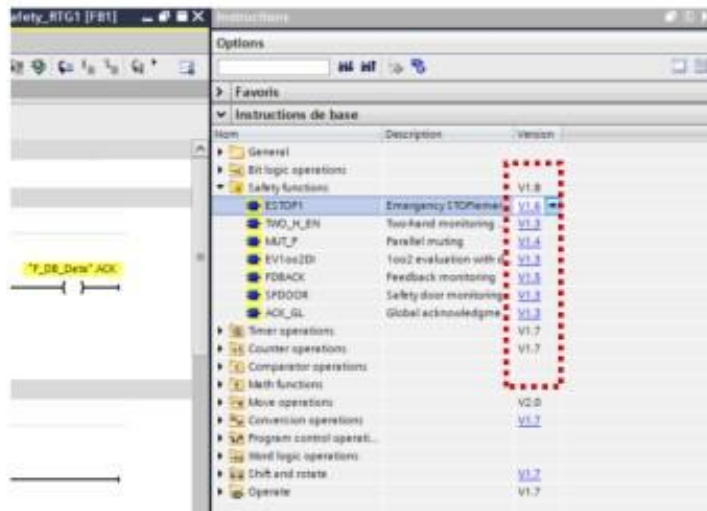
Si vous souhaitez étendre le programme de sécurité après migration du projet, nous vous recommandons avant la première compilation avec STEP 7 Safety Advanced V15, à la rubrique « Paramètres » (Settings) dans l'éditeur Safety Administration, de mettre à jour les éléments utilisés issus de la bibliothèque système dans le programme de sécurité, en veillant à utiliser la version logicielle la plus récente.

11.1.7. Versions du programme de sécurité (2)

Recommandation lors de la modification du programme de sécurité :

Avant la première compilation avec STEP 7 Safety Advanced V16, sélectionnez la version la plus récente disponible pour les instructions utilisées.

Veuillez tenir compte des remarques relatives aux versions des instructions.



En cas de changement de version d'une instruction, il faut compiler deux fois pour obtenir un programme de sécurité cohérent.

Dernière version pour les instructions

Si vous souhaitez étendre le programme de sécurité après sa migration, nous vous recommandons avant la première compilation avec STEP 7 Safety Advanced V15 de mettre à jour les instructions utilisées en veillant à utiliser la version logicielle la plus récente.

Compilation du programme de sécurité migré

En compilant le projet migré, la structure du programme (avec F-CALL) est transformée en structure STEP 7 Safety Advanced V13 (avec bloc principal de sécurité - Main Safety Block). La signature globale est alors modifiée et le programme de sécurité doit à nouveau faire l'objet d'une recette technique, le cas échéant.

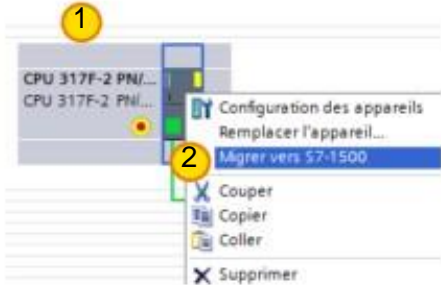
Remarque

Veillez à ce que lors de la compilation du programme de sécurité du projet migré, le temps d'exécution du/des groupe(s) d'exécution du programme de sécurité et la capacité mémoire du programme de sécurité soient étendues.

11.2. Migration de S7-300F vers S7-1500F

Ouvrir le projet avec le matériel « Classic » et compiler ①

Lancer la migration vers S7-1500 ②



Migration d'une CPU de sécurité pour automate S7-300F vers une CPU de sécurité pour S7-1500

Pour réaliser la migration d'une CPU S7-300/400F vers une CPU S7-1500F, il faut procéder comme pour faire migrer une CPU standard S7-300/400 vers une CPU standard S7-1500. Après la migration, il convient de tenir compte des éléments ci-dessous :

- Création d'un groupe d'exécution du programme de sécurité et affectation du bloc principal de sécurité (Main Safety Block).
- La configuration matérielle de la CPU d'origine (S7-300/400F) n'est pas automatiquement transmise à la CPU cible (S7-1500F). Réalisez manuellement la configuration matérielle de la nouvelle CPU après la migration.

11.2.1. Instructions non admissibles

Instructions non prises en charge

- OV
- MUTING
- TWO_HAND
- WR_FDB
- RD_FDB
- OPN
- SENDS7
- RCVS7

Attention :

Si l'un des blocs du projet est utilisé avec une CPU de sécurité classique, la migration de l'API ne peut pas être effectuée. Veuillez à adapter les appels de blocs dans le projet.



Migration d'une CPU de sécurité pour automate S7-300F vers une CPU de sécurité pour S7-1500

Compilez le programme de sécurité et corrigez les erreurs de compilation signalées, le cas échéant.

Remarque

Une nouvelle réception est requise après la migration de la CPU F.

11.2.2. Modification de la programmation

Types de données non pris en charge

- DWORD

La communication des groupes d'exécution du programme de sécurité n'est pas prise en charge.

- Avec le S7-1500, l'échange de données entre les deux groupes d'exécution du programme de sécurité est à ce jour impossible.

Modification des noms des DB de la périphérie de sécurité

- Les noms symboliques des DB de la périphérie de sécurité changent après la migration. Les noms doivent être copiés manuellement aux différentes occurrences dans le programme.



Modification de la programmation du programme de sécurité

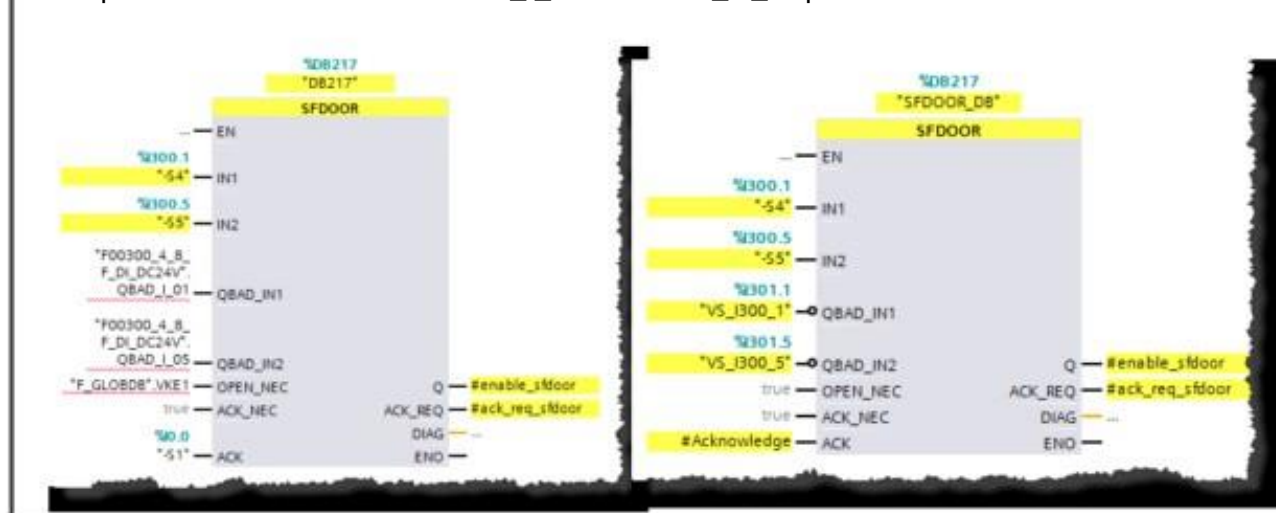
- Remplacement du F_GLOBDB.VKE0/1 par FALSE/TRUE.
- Remplacement des valeurs lisibles de F_GLOBDB pour le DB d'information du groupe d'exécution du programme de sécurité.
- Remplacement de la variable QBAD_I_xx ou QBAD_O_xx par l'état de la valeur.

La communication des groupes d'exécution du programme de sécurité n'est pas assurée.

11.2.3. Modification des fonctions de sécurité (1)

Programmation modifiée du programme de sécurité

- Remplacement de F_GLOBDB.VKE0/1 par FALSE/TRUE
- Remplacement des valeurs lisibles de F_GLOBDB par le DB d'information sur le groupe d'exécution du programme de sécurité.
- Remplacement de la variable QBAD_I_xx ou QBAD_O_xx par l'état de la valeur.



11.2.4. Modification des fonctions de sécurité (2)

Instructions non converties

• Les fonctions ont été étendues et peuvent être reproduites à l'identique avec les nouvelles fonctions. L'adaptation requise doit être effectuée manuellement.

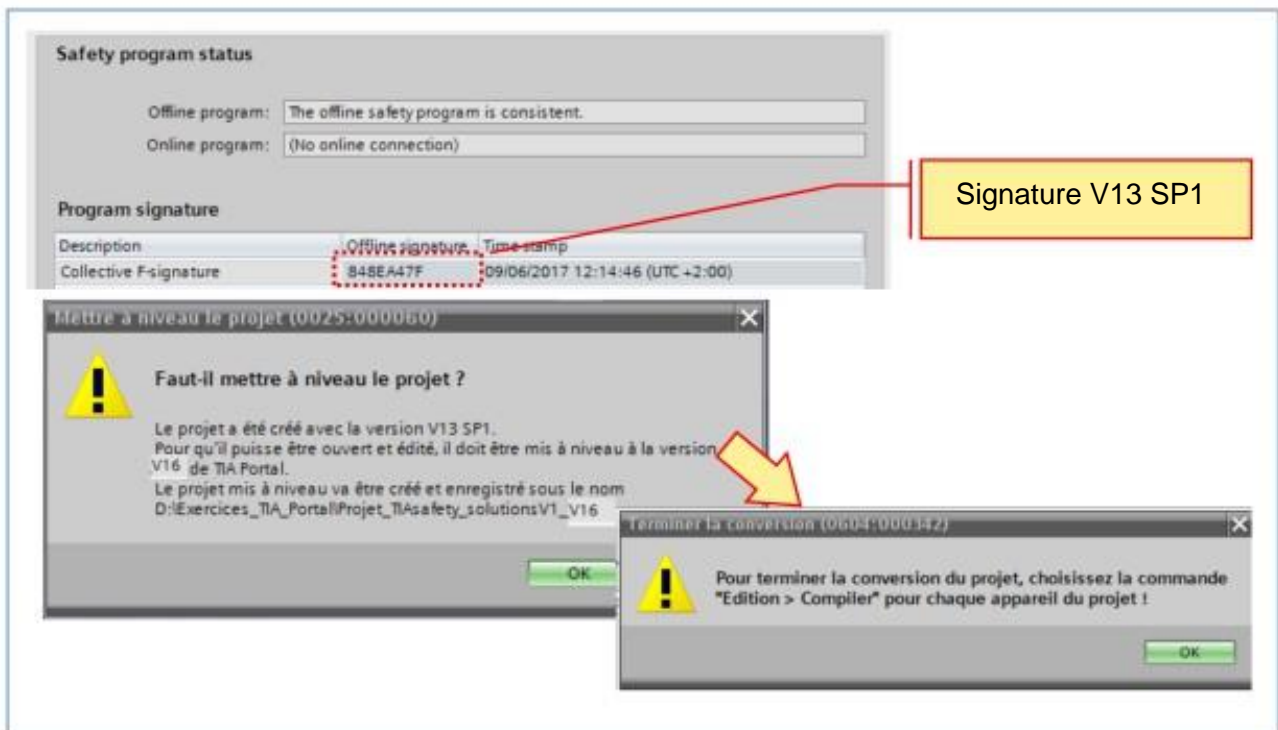
- MUTING → MUT_P (MUT_P propose également une fonction d'inhibition temporaire de la fonction de protection)



- TWO_HAND → TWO_H_EN (avec une entrée de validation supplémentaire)



11.3. Mettre à niveau des projets STEP 7 Safety V13 SP1 en V16



Si vous souhaitez étendre un projet issu de STEP 7 Safety V13 SP1, vous devez mettre le projet à niveau en version STEP 7 Safety V16.

Procédez à la mise en niveau, comme c'est l'usage dans STEP 7. Après la mise à niveau en V16, vous devez compiler votre programme de sécurité.

(S7-300/400) : Après la compilation, votre programme de sécurité est cohérent et la signature globale du programme de sécurité migré correspond à la signature globale de sécurité dans V13 SP1. Il est inutile de procéder à la recette des modifications.

11.3.1. Nouvelle compilation

!

Program was migrated from V13 SPx to V16. See [F-convert log](#) for system-related changes of the collective F-signature.

General

F-runtime group

F-runtime group 1 [RTG1]

F-blocks

F-compliant PLC data types

Access protection

Web server F-admins

Settings

Flexible F-Link

General

Safety mode status

Current mode: (No online connection)

Disable safety mode

Safety program status

Offline program: The offline safety program is inconsistent.

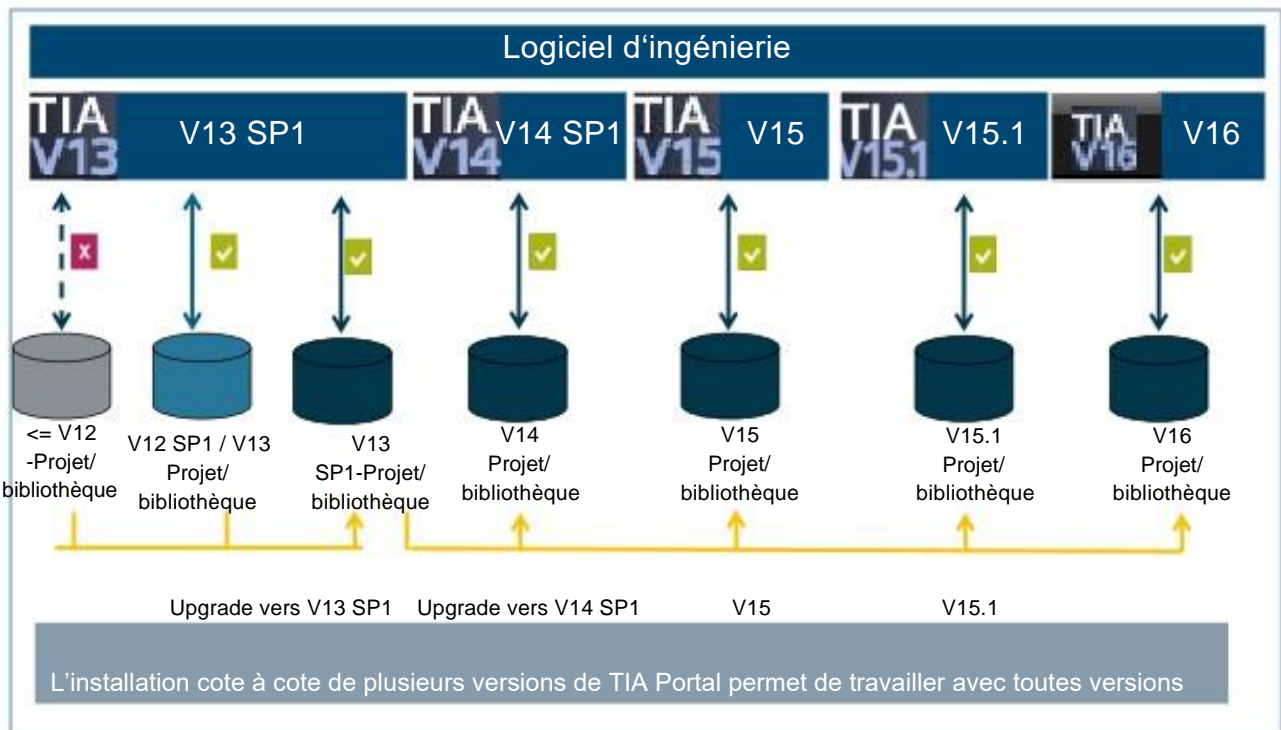
Online program: (No online connection)

Signatures

Signature	Offline signature	Time stamp
Collective F-signature	none	none
Software F-signature	none	
Hardware F-signature	none	
F-communication address signature	none	

Le programme de sécurité doit être compilé

11.4. Mettre à niveau des projets STEP 7 Safety antérieurs à V13 SP1



Les projets antérieurs doivent être mis à niveau en version V13SP1/SP2, à l'aide de la Version V13SP1/SP2, qui peut être installée en parallèle (mode dual) avec la V16.